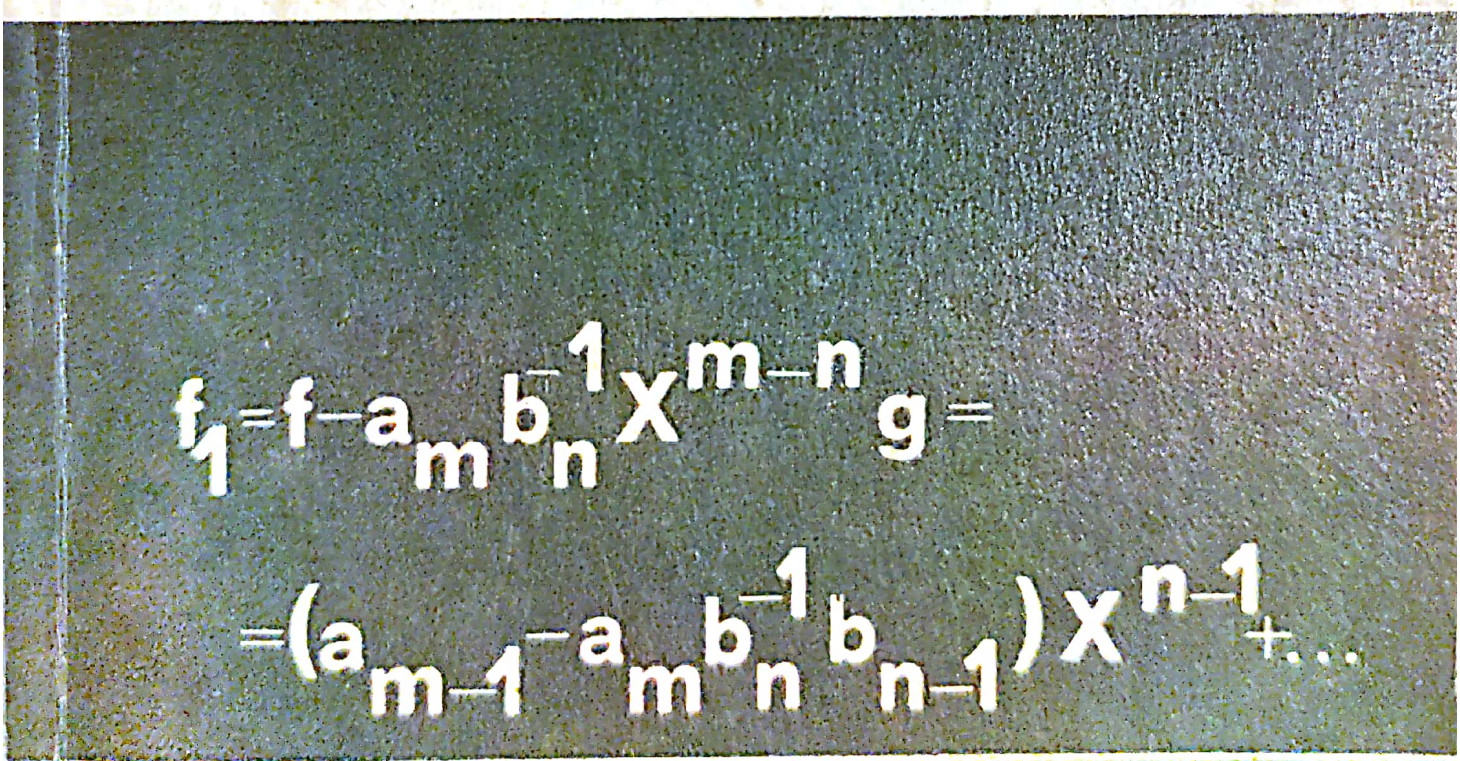
Ion D. Ion
C. Niță

Elemente de aritmetică cu aplicații în tehnici de calcul



Scanned with OKEN Scanner

ION D. ION
CONSTANTIN NIȚĂ

Elemente de aritmetică cu aplicaţii în tehnici de calcul

EDITURA TEHNICĂ
Bucureşti — 1978

Scanned with OKEN Scanner

Cartea prezintă principalele metode algoritmice din aritmetica elementară. Sînt analizate o serie de probleme actuale ale aritmeticii, apărute în esență datorită renunțării treptate la metoda tradițională de calcul „cu creionul și hîrtia" și folosirii în acest scop a calculatoarelor cu program.

Alături de algoritmii clasici ca algoritmul lui Euclid, ciurul lui Eratostene, algoritmul sistemelor de numerație, în carte sînt prezentate metode de calcul recent descoperite, ca algoritmul binar, metoda Garner de conversiune a numerelor din reprezentarea modulară, metoda Schönhage de înmulțire a numerelor mari. Cartea conține și un important capitol al analizei diofantice — soluții întregi ale sistemelor liniare, capitol ce constituie principalul instrument pentru programarea liniară în numere întregi.

În carte sînt date toate elementele de aritmetică necesare discutării problematicii abordate, fiind astfel accesibilă oricărui cititor cu o pregătire matematică medie. Ea este utilă profesorilor din învățămîntul gimnazial și liceal, elevilor din liceu, programatorilor, studenților, inginerilor și economiștilor interesați în metode actuale de calcul.

Scanned with OKEN Scanner

Cuprins

Cap. I. **Elemente de teoria mulțimilor** 5
§ 1. Mulțimi și funcții. 5
§ 2. Operații algebrice. 10
§ 3. Relații de echivalență 14
Cap. II. **Mulțimi de numere** 20
§ 1. Construcția numerelor naturale 20
§ 2. Elemente de aritmetică în $\mathbb{N}$ 29
§ 3. Construcția numerelor întregi 34
§ 4. Construcția numerelor raționale. 49
§ 5. Structuri algebrice. 66
§ 6. Inele de polinoame 75
Cap. III. **Inele euclidiene** 81
§ 1. Definiția inelelor euclidiene. Exemple 81
§ 2. Divizibilitate în domenii de integritate 86
§ 3. C.m.m.d.c. în inele euclidiene. 91
§ 4. Algoritmul lui Euclid 96
§ 5. Algoritmi. 100
§ 6. Sisteme de numerație 107
§ 7. Algoritmul binar 124
Cap. IV. **Inele cu descompunere unică în factori primi** 130
§ 1. Inele factoriale 130
§ 2. Elemente ireductibile în inele de polinoame 136
§ 3. Metode algoritmice pentru descompunerea numerelor în factori primi 144
Cap. V. **Aritmetică modulară** 159
§ 1. Inelul claselor de resturi modulo n 159
§ 2. Elemente de ordin finit într-un grup 165
§ 3. Teorema lui Lagrange. Consecințe 169
§ 4. Congruențe 173
§ 5. Lema chinezească a resturilor 182
§ 6. O metodă de înmulțire a numerelor naturale mari . . . 188
Cap. VI. **Rezolvarea în numere întregi a sistemelor de ecuații liniare** 200
§ 1. Matrice elementare 200
§ 2. Matrice aritmetic echivalente 207
§ 3. Soluții întregi ale unui sistem de ecuații liniare 215
Bibliografie 230

Scanned with OKEN Scanner

Prefață

Obiectivul principal al cărții este prezentarea metodelor algoritmice ale aritmeticii elementare. Interesul față de acest subiect al aritmeticii se explică prin tendința actuală de renunțare la metoda tradițională de calcul „cu creionul și hîrtia" și folosirii în acest scop a calculatoarelor cu program.

Pentru a crea cadrul teoretic necesar înțelegerii corecte a metodelor algoritmice expuse precum și pentru a mări gradul de independență a lucrării, sînt prezentate o serie de elemente de aritmetică: construcția numerelor naturale, întregi și raționale (cap. II), aritmetică în mulțimea numerelor naturale (cap. II), inele cu algoritmul lui Euclid (cap. III), inele cu descompunere unică în factori primi (cap. IV), teoria congruențelor și lema chinezească a resturilor (cap. V), teorema factorilor invarianți (cap. VI).

O serie de algoritmi clasici, cum sînt algoritmul lui Euclid, ciurul lui Eratostene, algoritmul sistemelor de numerație, algoritmi pentru descompunerea numerelor în factori primi sînt analizați și redactați în ideea executării lor pe un calculator cu program.

Actuala tendință a tehnicii de calcul a revitalizat o serie de capitole de aritmetică, a pus acesteia numeroase probleme, multe dintre ele doar parțial rezolvate. Dintre rezultatele recente obținute în acest sens, în carte este prezentat algoritmul binar pentru calculul celui mai mare divizor comun a două numere întregi, metoda Garner de conversiune a numerelor din reprezentarea modulară, metoda Schönhage de înmulțire a numerelor mari.

Ultimul capitol prezintă un subiect al analizei diofantice — rezolvarea în numere întregi a sistemelor de ecuații liniare. Rezultatele din acest capitol dau instrumentul de bază pentru programarea liniară în numere întregi.

Autorii

Scanned with OKEN Scanner

CAPITOLUL I

Elemente de teoria mulțimilor

§ 1. Mulțimi și funcții

Se vor face cîteva referiri scurte la unele noțiuni de teoria mulțimilor care intervin în această carte.

Fie E o mulțime (colecție) de elemente. Faptul că un element x aparține mulțimii E se indică prin $x \in E$, iar negația sa se scrie $x \notin E$. Dacă E și F sînt două mulțimi, se spune că E este o submulțime a lui F, sau că este inclusă în F, dacă oricare ar fi $x \in E$, atunci $x \in F$. Dacă E este inclus în F, se scrie $E \subset F$. Simbolic, putem scrie aceasta prin $x \in E \Rightarrow x \in F$, unde $\Rightarrow$ se citește „implică". Egalitatea $E = F$ este echivalentă cu $E \subset F$ și $F \subset E$ (simbolic, $E = F \Leftrightarrow E \subset F$ și $F \subset E$, unde $\Leftrightarrow$ se citește „dacă și numai dacă"). Dacă $E \subset F$ și $E \neq F$, se spune că E este submulțime proprie a lui F sau că E este inclusă strict în F și se scrie $E \subsetneq F$.

Dacă E este o mulțime, atunci mulțimea submulțimilor lui E (inclusiv submulțimea vidă a lui E, notată $\emptyset$), se notează cu $P(E)$ și se numește *mulțimea părților mulțimii* E. O submulțime a lui E se va specifica printr-o proprietate sau mai multe proprietăți. Pentru a indica aceasta, scriem

$$A = \{x \in E \mid \ldots\}$$

Scanned with OKEN Scanner

(sau, dacă E este fixată, $A = \{x \mid \ldots\}$ unde la ... se înşiră proprietăţile care caracterizează A. De exemplu, dacă $\mathbb{Z}$ este mulţimea numerelor întregi, atunci $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geqslant 0\}$ defineşte submulţimea numerelor întregi nenegative, adică mulţimea numerelor naturale.

Dacă A şi B sînt submulţimi ale mulţimii E, submulţimea lui E formată din elementele x astfel că $x \in A$ şi $x \in B$ se numeşte *intersecţia lui A cu B*. Această submulţime se notează $A \cap B$. Deci

$$A \cap B = \{x \in E \mid x \in A \text{ şi } x \in B\}.$$

Reuniunea $A \cup B$ a submulţimilor A şi B este submulţimea mulţimii E formată din elementele x, astfel încît $x \in A$ sau $x \in B$, adică

$$A \cup B = \{x \in E \mid x \in A \text{ sau } x \in B\}.$$

Sînt bine cunoscute o serie de proprietăţi referitoare la $\cap$ şi $\cup$, de aceea nu le vom menţiona aici.

Fie acum E şi F două mulţimi. Se defineşte *produsul (cartezian)* al lui E cu F, notat $E \times F$, ca fiind mulţimea perechilor distincte (x, y) cu $x \in E$ şi $y \in F$, adică

$$E \times F = \{(x, y) \mid x \in E \text{ şi } y \in F\}.$$

În $E \times F$ două elemente (x, y) şi (x', y') sînt egale dacă şi numai dacă $x = x'$ şi $y = y'$. Dacă E este formată din m elemente $x_1, x_2, \ldots, x_m$ iar F este formată din n elemente $y_1, y_2, \ldots, y_n$, atunci $E \times F$ este formată din mn elemente şi anume (x_i, y_j), $i = 1, 2, \ldots, m$; $j = 1, 2, \ldots, n$.

Definiţia 1.1. O *funcţie* de la o mulţime E la o mulţime F constă dintr-o mulţime E numită *domeniu* (de definiţie) al funcţiei, o mulţime F numită *codomeniu* şi o submulţime f a produsului cartezian $E \times F$ numită *graficul funcţiei*, care are următoarele proprietăţi:

1) pentru orice $x \in E$ există $y \in F$ astfel încît $(x, y) \in f$;

2) dacă $(x, y), (x', y') \in f$, atunci $y = y'$.

Scanned with OKEN Scanner

Funcţia f de la E la F se notează prin $f : E \to F$ sau $E \xrightarrow{f} F$.

Observaţie. În cazul definirii unei funcţii, faptul că „funcţia este bine definită" înseamnă că condiţia 2) să fie adevărată. Împreună, condiţiile 1) şi 2) înseamnă că pentru fiecare $x \in E$ există un unic $y \in F$, astfel încît $(x, y) \in f$. Notaţia clasică pentru acest element y este $f(x)$ şi se numeşte *imaginea* lui x prin f.

Uneori cuvîntul „funcţie" este înlocuit cu „aplicaţie".

Fie $f : E \to F$ o funcţie. Dacă A este o submulţime a lui E, atunci mulţimea $\{f(x) \mid x \in A\}$ se notează cu $f(A)$ şi se numeşte *imaginea* lui A prin f. În particular, $f(E)$ se numeşte *imaginea funcţiei* f şi se notează încă Im f. Dacă B este o submulţime a lui F, atunci mulţimea $f^{-1}(B) = \{x \in E \mid f(x) \in B\}$ se notează cu $f^{-1}(B)$ şi se numeşte *imaginea reciprocă* a lui B prin f.

Cînd domeniul şi codomeniul sînt subînţelese, se spune, simplu, funcţia f (sau aplicaţia f), dar, corect spus, f este doar o componentă a funcţiei.

Dacă E' este o submulţime a lui E şi f o funcţie de la E la F, atunci funcţia de la E' la F al cărei grafic este submulţimea lui $E' \times F$ formată din elementele $(x', f(x'))$, $x' \in E'$, se numeşte *restricţia funcţiei* f la E' şi se notează prin $f|_{E'}$. Invers, se spune că funcţia f de la E la F este o *extensie* a funcţiei g de la E' la F, dacă $g = f|_E$.

O funcţie $f : E \to F$ se numeşte *surjectivă* dacă Im $f = F$, adică imaginea coincide cu codomeniul său. Funcţia $f : E \to F$ este *injectivă* dacă elemente diferite din E au imagini diferite în F, adică dacă $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. Dacă funcţia f este în acelaşi timp injectivă şi surjectivă, aceasta se numeşte *bijectivă* (sau, se spune că f este o corespondenţă biunivocă între E şi F).

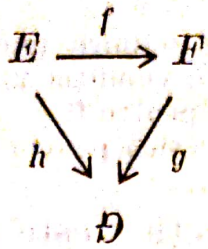
Fie $f : E \to F$ şi $g : F \to G$ două funcţii. Se defineşte $g \circ f : E \to G$ ca fiind funcţia care are domeniul E şi codomeniul G, iar graficul este submulţimea lui $E \times G$ formată din elementele $(x, g(f(x)))$, $x \in E$. Atunci prin definiţie

$$(g \circ f)(x) = g(f(x)).$$

Această funcţie se numeşte *compunerea funcţiei* f *cu funcţia* g. Se obişnuieşte să se indice relaţia $h = g \circ f$ prin aceea că

Scanned with OKEN Scanner

diagrama



este comutativă.

Pentru o mulțime E se definește *funcția identică* $\mathbf{1}_E$ (sau, simplu, $\mathbf{1}$ dacă E este fixată) ca $\mathbf{1}_E : E \to E$, unde $\mathbf{1}_E$ este submulțimea elementelor (x, x) ale lui $E \times E$. Această submulțime se numește *diagonala* lui $E \times E$. Dacă $f : E \to F$, este clar că $\mathbf{1}_E \circ f = f = f \circ \mathbf{1}_E$.

Funcția $f : E \to F$ se numește *inversabilă* dacă există o funcție $g : F \to E$, astfel încît $g \circ f = 1_E$ și $f \circ g = \mathbf{1}_F$.

Iată, acum, următorul rezultat important.

Propoziția 1.1. *O funcție este bijectivă dacă și numai dacă este inversabilă.*

Demonstrație. Presupunem că $f : E \to F$ este bijectivă. Fie submulțimea g a lui $E \times F$ formată din elementele $(f(x), x)$, $x \in E$. Dacă $y \in F$, din surjectivitatea lui f rezultă că există $x \in E$, astfel încît $f(x) = y$. Prin urmare, pentru mulțimea g a perechilor de forma $(f(x), x)$, $x \in E$, este adevărată condiția 1) de la definiția funcției. Datorită injectivității lui f, rezultă că g este „bine definită", adică condiția 2) este adevărată. Într-adevăr, dacă (y, x_1), $(y, x_2) \in g$, atunci $f(x_1) = y = f(x_2)$ și deci $x_1 = x_2$. Așadar, se obține o funcție $g : F \to E$. Dacă $x \in E$, din $(x, f(x)) \in f$ și $(f(x), x) \in g$ rezultă $g(f(x)) = x$; deci $g \circ f = \mathbf{1}_E$. Dacă $y \in F$, atunci $y = f(x)$, $x \in E$ și $(y, x) \in g$, adică $g(y) = x$. Prin urmare, $f(g(y)) = f(x) = y$; deci $f \circ g = \mathbf{1}_F$. Reciproc, presupunem că funcțiile $f : E \to F$ și $g : F \to E$ satisfac relațiile $g \circ f = \mathbf{1}_E$ și $f \circ g = \mathbf{1}_F$. Dacă $y \in F$, fie $x = g(y)$. Atunci $f(x) = f(g(y)) = y$ și deci f este surjectivă. Fie acum $f(x_1) = f(x_2)$, pentru $x_1, x_2 \in E$. Atunci $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$ și deci f este injectivă.

Scanned with OKEN Scanner

Funcţia f satisfăcînd $g \circ f = 1_E$ şi $f \circ g = 1_F$ este unică. Într-adevăr, dacă $g' : F \to E$ satisface aceleaşi condiţii $g' \circ f = 1_E$ şi $f \circ g' = 1_F$, atunci

$$g' = 1_F \circ g' = (g \circ f) \circ g' = g \circ (f \circ g') = g \circ 1_E = g.$$

Funcţia g se notează, de obicei, cu f^{-1} şi se numeşte *inversa funcţiei* (bijective) f. Este clar că, de asemenea, f^{-1} este bijectivă şi $(f^{-1})^{-1} = f$.

Propoziţia 1.2. *Compunerea a două funcţii bijective este o funcţie bijectivă.*

Demonstraţie. Dăm o demonstraţie în care se aplică criteriul de bijectivitate. Fie pentru aceasta $f : E \to F$ şi $g : F \to G$ două funcţii bijective şi inversele lor $f^{-1} : F \to E$ şi $g^{-1} : G \to F$, precum şi compunerea $f^{-1} \circ g^{-1} : G \to E$. Atunci

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = ((g \circ f) \circ f^{-1}) \circ g^{-1} = g \circ (f \circ f^{-1}) \circ g^{-1} =$$
$$= g \circ g^{-1} = 1_G$$

şi

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ (g \circ f)) = f^{-1} \circ (g^{-1} \circ g) \circ f =$$
$$= f^{-1} \circ f = 1_E.$$

Deci $f^{-1} \circ g^{-1}$ este inversa funcţiei $g \circ f$, adică

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Definiţia 1.2. Fie X şi I două mulţimi. Se numeşte *familie de elemente din mulţimea X, indexată după mulţimea I*, o aplicaie $f : I \to X$. Mulţimea I se numeşte mulţimea de indici a familiei f.

Dacă se pune $f(i) = x_i$, atunci familia de elemente f se notează $(x_i)_{i \in I}$.

Dacă elementele lui X sînt mulţimi, atunci termenul de familie de elemente se înlocuieşte cu familie de mulţimi, iar $f(i)$ se notează X_i. Fie E o mulţime şi $X = P(E)$

Scanned with OKEN Scanner

mulţimea părţilor lui E. În acest caz, termenul de familie de elemente din X se înlocuieşte cu familie de submulţimi (părţi) ale lui E.

Ca şi pentru două mulţimi pot fi definite reuniunea şi intersecţia unei familii oarecare de mulţimi, acestea avînd o serie de proprietăţi, dealtfel, cunoscute. Nu vom insista asupra lor.

§ 2. Operaţii algebrice

Conceptul de produs cartezian a două mulţimi permite definirea noţiunii de *funcţie de două variabile.* Astfel, o funcţie de două variabile definită pe E cu valori în F este o funcţie de la $E \times E$ în F.

Definiţia 2.1. Dacă E este o mulţime, se numeşte *operaţie algebrică* (internă) sau *lege de compoziţie* (internă), pe E, orice funcţie φ de două variabile pe E cu valori în E, adică o funcţie φ definită pe $E \times E$ cu valori în E:

$$\varphi : E \times E \to E, \qquad (x, y) \to \varphi(x,y).$$

Pentru a simplifica notaţia se scrie $\varphi(x, y)$ în loc de $\varphi((x, y))$. În cele ce urmează, nu mai intervin şi alte operaţii algebrice în afară de cele interne, aşa că se va spune, pe scurt, operaţie algebrică în loc de operaţie algebrică internă.

Se va nota cu $\mathbb{N}$ mulţimea numerelor naturale, cu $\mathbb{Z}$ mulţimea numerelor întregi, cu $\mathbb{Q}$ mulţimea numerelor raţionale, cu $\mathbb{R}$ mulţimea numerelor reale iar cu $\mathbb{C}$ mulţimea numerelor complexe.

În continuare, ne vom ocupa, pe larg, de primele trei mulţimi şi anume: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, totuşi deocamdată considerăm cunoscute unele proprietăţi ale lor.

Exemple de operaţii algebrice

1. Pe mulţimile $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ adunarea şi înmulţirea sînt operaţii algebrice.

2. Reuniunea şi intersecţia pe mulţimea $P(T)$ a părţilor unei mulţimi T sînt operaţii algebrice.

Scanned with OKEN Scanner

3. Fie E o mulțime și $F(E)$ mulțimea funcțiilor definite pe E cu valori în E. Compunerea funcțiilor este o operație algebrică pe $F(E)$.

4. Dacă T este o mulțime, funcțiile (proiecții) $p_1 : T \times T \to T$, definită prin $p_1(x, y) = x$, și $p_2 : T \times T \to T$, definită prin $p_2(x, y) = y$, sînt operații algebrice pe T.

5. Pe mulțimea $\mathbb{Z}$ a numerelor întregi, scăderea este operație algebrică. De asemenea, scăderea pe $\mathbb{Q}$, $\mathbb{R}$ sau $\mathbb{C}$ este o operație algebrică. Însă pe mulțimea $\mathbb{N}$ aceasta nu este operație algebrică, deoarece rezultatul scăderii a două numere naturale nu este întotdeauna un număr natural.

Observație. Dacă φ este o operație algebrică pe mulțimea E în loc de $\varphi(x, y)$ se va scrie $x\varphi y$ și se va citi *compusul* lui x cu y prin operația φ (sau, x compus cu y). Operația algebrică se poate nota în mai multe feluri, citind aceasta în mod diferit. Dacă se notează cu $+(x, y) = x + y$, se citește *suma* lui x cu y (sau x adunat cu y) sau dacă se notează cu $\cdot(x, y) = xy$, se citește *produsul* lui x cu y (sau x înmulțit cu y).

În cele ce urmează, în loc de operație algebrică se va spune *operație*, deoarece nu vor fi alte tipuri de operații.

Pentru orice operație $\varphi : E \times E \to E$ elementul $\varphi(x, y)$ din E, corespunzător perechii (x, y), se va nota prin $x * y$.

Se dau, mai jos, cîteva proprietăți ale operațiilor algebrice, cu ajutorul cărora se definesc structurile de bază ale algebrei.

— *Asociativitatea.* Fie E o mulțime și $* : E \times E \to E$ o operație pe mulțimea E. Se spune că operația $*$ este *asociativă* dacă, oricare ar fi elementele x, y, z din E, are loc egalitatea

$$x * (y * z) = (z * y) * z.$$

1. Adunarea și înmulțirea în $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sînt operații asociative.

2. În $P(T)$ reuniunea și intersecția sînt operații asociative.

3. Compunerea funcțiilor pe $F(E)$ este operație asociativă.

4. Operațiile proiecții sînt asociative. De exemplu, să verificăm pentru p_1: $(x * y) * z = p_1(p_1(x, y), z) = p_1(x, z) = x$ și $x * (y * z) = p_1(x, p_1(y, z)) = p_1(x, y) = x$.

5. Scăderea numerelor întregi (raționale, reale, complexe) nu este operație asociativă.

De exemplu: $5 - (7 - 3) = 1 \neq -5 = (5 - 7) - 3$.

— *Comutativitatea.* Se spune că o operație $*$ definită pe o mulțime E este *comutativă* dacă, oricare ar fi elementele x, y din E, are loc egalitatea

$$x * y = y * x.$$

Scanned with OKEN Scanner

Exemple

1. Adunarea și înmulțirea pe $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sînt operații comutative.

2. În $P(T)$ reuniunea și intersecția sînt comutative.

3. Compunerea funcțiilor pe $F(E)$ nu este, în general, comutativă. Se poate verifica cu ușurință că ea este comutativă, dacă și numai dacă E are un singur element.

4. Operațiile proiecții sînt necomutative.

Să verificăm de exemplu, pentru p_1. Dacă $x \neq y$, atunci

$$x * y = p_1(x, y) = x$$

iar

$$y * x = p_1(y, x) = y.$$

Cum $x \neq y$, rezultă $x * y \neq y * x$.

5. Operația de scădere în $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ este necomutativă.

— *Element neutru.* Se spune că elementul $e \in E$ este *element neutru* (*unitate*) pentru operația $* : E \times E \to E$ dacă, oricare ar fi $x \in E$, $x * e = e * x = x$.

Exemple

1. Numărul 0 (respectiv 1) este element neutru pentru adunarea (respectiv înmulțirea) în $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

2. În $P(T)$, mulțimea vidă $\emptyset$ este element neutru pentru reuniune, iar T pentru intersecție.

3. Funcția identică $1_E : E \to E$ este element neutru pentru compunerea funcțiilor pe $F(E)$.

4. Pentru operațiile definite de proiecții nu există element neutru. Să arătăm pentru p_1. Într-adevăr, dacă $e \in T$ ar fi element neutru, atunci pentru $x \in T$ rezultă $x * e = x$ și $e * x = e$. Dar egalitatea $x = e$ nu are loc pentru orice $x \in T$, dacă presupunem că T are cel puțin două elemente.

În legătură cu elementul neutru al unei operații, are loc următorul rezultat.

Propoziția 2.1. *Orice operație algebrică admite cel mult un element neutru.*

Demonstrație. Să presupunem că operația $*$ are două elemente neutre e și e' și va rezulta $e = e'$. Deoarece e este element neutru, atunci $e * e' = e'$. Apoi, cum e' este element neutru, rezultă $e * e' = e$. Deci $e = e'$.

Scanned with OKEN Scanner

Elementul neutru se mai numește *elementul unitate* atunci cînd operația este notată multiplicativ și *elementul zero* cînd operația este notată aditiv.

— *Elemente simetrizabile.* Fie $* : E \times E \to E$ o operație algebrică cu element neutru e și $x \in E$. Se spune că x este *simetrizabil* în raport cu operația dată, dacă există un element $x' \in E$, astfel încît $x * x' = x' * x = e$.

Elementul x' se numește *simetricul* lui x. În notația multiplicativă a operației algebrice x' se mai numește *inversul* lui x iar în notația aditivă a operației se mai numește *opusul* lui x.

Referindu-ne la exemplele de operații de mai înainte, se observă că în raport cu adunarea în $\mathbb{Z}$, opusul elementului m este $-m$; în raport cu înmulțirea în $\mathbb{Z}$ elementele inversabile sînt $+1$ și -1, iar toate celelalte numere întregi nu sînt inversabile.

Elementele inversabile din $F(E)$ sînt funcțiile bijective. Pentru operațiile definite de proiecții nu se pune problema, deoarece nu există element neutru.

Propoziția 2.2. *Fie $* : E \times E \to E$ o operație asociativă și cu element neutru e. Dacă elementul $x \in E$ este simetrizabil, atunci simetricul său este unic.*

Demonstrație. Fie x' și x'' două elemente din E, astfel încît $x * x' = x' * x = e$ și $x * x'' = x'' * x = e$. Atunci $x'' * (x * x') = x'' * e = x''$. Pe de altă parte, $x'' * (x * x') = (x'' * x) * x' = e * x' = x'$. Deci $x' = x''$.

Pentru o operație multiplicativă, inversul elementului x se notează cu x^{-1}, iar pentru cea aditivă se notează cu $-x$.

Propoziția 2.3. *Fie E o mulțime înzestrată cu operația $*$ și care admite element neutru e. Dacă $x, y \in E$ sînt simetrizabile, atunci $x * y$ este simetrizabil și*

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Demonstrație. $(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e$ și analog $(y^{-1} * x^{-1}) * (x * y) = e$. Deci $y^{-1} * x^{-1}$ este simetricul elementului $x * y$, adică $(x * y)^{-1} = y^{-1} * x^{-1}$.

Scanned with OKEN Scanner

Fie E o mulțime. Se spune că pe E este definită o *relație binară*, dacă este dată o submulțime R a produsului cartezian $E \times E$. Elementele $x, y \in E$ sînt în relația R și scriem xRy dacă $(x, y) \in R$. O relație binară poate avea una sau mai multe dintre proprietățile următoare:

1° Pentru orice $x \in E$, avem xRx (*reflexivitate*).

2° Dacă $x, y \in E$ și xRy, atunci yRx (*simetrie*).

3° Dacă $x, y \in E$, din xRy și yRx rezultă $x = y$ (*antisimetrie*).

4° Dacă $x, y, z \in E$, din xRy și yRz rezultă xRz (*tranzitivitate*).

Relațiile binare se clasifică după proprietățile pe care le au. Cele mai importante relații binare sînt următoarele: relațiile care au proprietățile 1° și 4°, adică sînt reflexive și tranzitive, numite *relații de cvasiordine* (*preordine*); relațiile care au proprietățile 1°, 3° și 4°, adică sînt reflexive, antisimetrice și tranzitive, numite *relații de ordine* (parțială); relații care au proprietățile 1°, 2° și 4°, adică sînt reflexive, simetrice și tranzitive, numite *relații de echivalență*.

O mulțime nevidă E împreună cu o relație R de ordine (parțială) pe E se numește *mulțime* (parțial) *ordonată*. În acest caz, de obicei, relația se notează cu $\leqslant$, adică $x \leqslant y$ dacă și numai dacă $(x, y) \in R$ și se citește „x mai mic sau egal cu y". Astfel de relații vor apărea în paragrafele referitoare la numere.

Se spune că o mulțime ordonată E este *total ordonată* dacă, oricare ar fi $x, y \in E$, $x \leqslant y$ sau $y \leqslant x$. O mulțime ordonată se numește *bine ordonată*, dacă oricare ar fi partea nevidă F a sa există $z \in F$ astfel încît $z \leqslant x$ pentru orice $x \in F$. (Orice parte nevidă a sa are un cel mai mic element).

Relațiile de echivalență vor avea un rol important în cele ce urmează.

Dacă R este o relație de echivalență pe mulțimea E și $(x, y) \in R$, atunci scriem $x \sim_R y$, sau chiar $x \sim y$ și citim „x echivalent cu y". Dacă $(x, y) \notin R$, scriem $x \nsim y$ și citim „x nu este echivalent cu y".

Scanned with OKEN Scanner

Exemple

1. Fie E mulțimea tuturor locuitorilor unui oraș și R mulțimea tuturor perechilor ordonate (x, y) cu proprietatea „locuitorul x este născut în același an cu locuitorul y". Evident, R este o relație de echivalență pe E.

2. Fie E mulțimea punctelor din planul P și definim relația R astfel: dacă $x, y \in E$, atunci xRy dacă x și y se găsesc pe aceeași dreaptă verticală, Evident R este o relație de echivalență.

3. Fie mulțimea E de la exemplul 2 și fixăm un punct O numit origine, în planul P. Două puncte $x, y \in E$ sînt în relația R' dacă se găsesc pe același cerc cu centrul în O. Deci R' este relație de echivalență.

4. Fie E mulțimea dreptelor în planul P. Se definește relația R astfel: dacă $x, y \in E$, atunci xRy dacă $x \| y$ (x este paralelă cu y). Trebuie remarcat că prin sensul care se dă aici paralelismului, o dreaptă este paralelă cu ea însăși. Este evident că această relație este de echivalență.

Definiția 3.1. Fie R o relație de echivalență pe mulțimea E. O submulțime nevidă C a lui E se numește *clasă de echivalență* a relației de echivalență R dacă:

1) $x, y \in C \Rightarrow x \sim_R y$,

2) $z \in E$, $x \in C$ și $z \sim_R x \Rightarrow z \in C$.

Propoziția 3.1. *Fie R o relație de echivalență pe mulțimea E și $x \in A$. Atunci:*

1) *Mulțimea $\hat{x} = \{y \in E \mid y \sim_R x\}$ este o clasă de echivalență.*

2) *Dacă C este o clasă de echivalență, atunci $C = \hat{x}$, oricare ar fi $x \in C$.*

Demonstrație. 1) Cum $x \sim_R x$, rezultă că $x \in \hat{x}$ și deci $\hat{x}$ este o submulțime nevidă. Dacă $y, z \in \hat{x}$, atunci $y \sim_R x$ și $z \sim_R x$. Deci $y \sim_R x$ și $x \sim_R z$, de unde $y \sim_R z$, căci relația de echivalență este tranzitivă. Așadar, $\hat{x}$ verifică 1). Fie $y \in \hat{x}$ și $z \in E$ astfel încît $z \sim_R y$. Atunci cum și $y \sim_R x$, rezultă $z \sim_R x$, deci $z \in \hat{x}$, așadar $\hat{x}$ verifică 2).

2) Dacă $x \in C$ și $y \in \hat{x}$, atunci $y \sim_R x$. După 2) rezultă $y \in C$ și deci $\hat{x} \subset C$. Dacă $y \in C$, atunci după 1) $y \sim_R x$, adică $y \in \hat{x}$, de unde $C \subset \hat{x}$. Așadar, $C = \hat{x}$.

Scanned with OKEN Scanner

Dacă $x \in E$, atunci $\hat{x}$ se numește *clasa de echivalență de reprezentant* x. Din propoziția precedentă rezultă că dacă C este o clasă de echivalență, orice element x al său este un reprezentant al lui C (adică $C = \hat{x}$), deci nici un element din C nu este „privilegiat" în privința reprezentării lui C.

Să ne oprim asupra exemplelor de mai înainte. Pentru relația de echivalență de la exemplul 1 mulțimea tuturor locuitorilor născuți în același an (dacă nu este vidă) este evident o clasă de echivalență. În al doilea exemplu, clasa de echivalență a punctului x din plan este dreapta verticală care trece prin x. În exemplul 3, clasa de echivalență a unui punct x din plan în raport cu relația R' este cercul cu centrul în origine și care conține pe x. În exemplul 4 clasa de echivalență a unei drepte x (adică mulțimea dreptelor paralele cu x) ne dă o direcție în plan. Deci mulțimea claselor este tocmai mulțimea direcțiilor din plan.

Propoziția 3.2. *Fie R o relație de echivalență pe o mulțime E și C, C' două clase de echivalență ale acestei relații. Dacă $C \neq C'$, atunci $C \cap C' = \emptyset$.*

Demonstrație. Dacă $C \cap C' \neq \emptyset$, fie $x \in C \cap C'$. Atunci după propoziția precedentă, rezultă $C = \hat{x} = C'$, ceea ce contrazice ipoteza.

Corolar 3.3. *Fie R o relație de echivalență pe E și x, y două elemente ale lui E. Atunci $\hat{x} = \hat{y}$ dacă și numai dacă $x \sim_R y$.*

Demonstrație. Dacă $\hat{x} = \hat{y}$, atunci $x \in \hat{x} = \hat{y}$, deci $x \in \hat{y}$, de unde $x \sim_R y$. Reciproc, dacă $x \sim_R y$, atunci $x \in \hat{y}$. Dar $x \in \hat{x}$ și deci $\hat{x} \cap \hat{y} \neq \emptyset$, de unde $\hat{x} = \hat{y}$.

Definiția 3.2. Fie R o relație de echivalență pe mulțimea E. O familie $\{x_i\}_{i \in I}$ de elemente din E se numește *sistem complet de reprezentanți* pentru relația de echivalență R:

1) dacă $i \neq j$, atunci $x_i \not\sim_R x_j$;

2) oricare $x \in E$, există $i \in I$ astfel încît $x \sim_R x_i$.

Dacă $\{x_i\}_{i \in I}$ este un sistem complet de reprezentanți, atunci din corolarul 3.3 și 1) rezultă că $\hat{x}_i \cap \hat{x}_j = \emptyset$, pentru $i \neq j$ iar din 2) rezultă

$$E = \bigcup_{i \in I} \hat{x}_i \text{ (reuniune disjunctă).}$$

Scanned with OKEN Scanner

Este clar că un sistem complet de reprezentanți se obține luînd cîte un reprezentant din fiecare clasă de echivalență și numai unul.

Definiția 3.3. Dacă R este o relație de echivalență pe mulțimea E, atunci mulțimea

$$E/R \stackrel{\text{def}}{=} \{\hat{x} \mid x \in E\}$$

se numește *mulțimea factor* a lui E în raport cu R, iar aplicația

$$\varphi_R : E \to E/R, \text{ definită prin } \varphi_R(x) = \hat{x}$$

se numește *aplicația canonică* de la mulțimea E la mulțimea factor E/R.

Evident, φ_R este aplicație surjectivă. Se definesc, adesea, mulțimile factor ca partiții.

Definiția 3.4. Se numește *partiție* a mulțimii E o familie $\pi(E) = \{E_i\}_{i \in I}$ de submulțimi nevide ale mulțimii E, astfel încît

1) $E_i \cap E_j = \emptyset$, dacă $i \neq j$;

2) $\bigcup_{i \in I} E_i = E$.

Rezultă că orice relație de echivalență R pe o mulțime E determină o partiție E/R a lui E, ale cărei elemente sînt clasele de echivalență ale relației R.

Remarcăm că orice funcție induce o relație de echivalență pe domeniul său. Într-adevăr, fie $f : E \to F$ o funcție. Atunci ea definește o relație binară pe E, notată R_f, punînd $xR_f y$ dacă și numai dacă $f(x) = f(y)$. Este clar că R_f este relație de echivalență. Dacă $z \in F$, fie

$$f^{-1}(z) = \{x \in E \mid f(x) = z\}$$

Scanned with OKEN Scanner

imaginea reciprocă a lui z. Dacă $z \notin \mathrm{Im} f$, atunci $f^{-1}(z) = \emptyset$. Pe de altă parte, dacă $z = f(x)$, pentru un anumit $x \in E$, atunci $f^{-1}(z) = f^{-1}(f(x)) = \{y \mid f(y) = f(x)\} = \{y \mid y R_f x\}$ și aceasta este tocmai clasa de echivalență a elementului x, relativ la R_f. Deci

$$E/R_f = \{f^{-1}(z)\}_{z \in \mathrm{Im} f}.$$

Reciproc, dacă R este o relație de echivalență pe E, considerînd mulțimea factor E/R și $\varphi : E \to E/R$, este clar că $R = R_\varphi$ (adică, dacă $x, y \in E$, atunci $x \sim_R y \Leftrightarrow x \sim_{R_\varphi} y$).

Definiția 3.5. Fie E și F două mulțimi și R o relație de echivalență pe E. Se spune că o funcție $f : E \to F$ este *compatibilă* cu R, dacă din $x \sim_R y$ în E rezultă $f(x) = f(y)$.

De exemplu, fie P un plan și un punct O al său numit origine. Definim

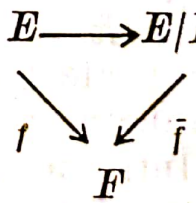
$$f : P \to \mathbb{R}, \text{ prin } f(x) = [\sqrt{\alpha^2 + \beta^2}], \qquad x = (\alpha, \beta)$$

(unde prin $[r]$ am desemnat partea întreagă a numărului real r)

$$g : P \to \mathbb{R}, \text{ prin } g(x) = \sqrt{\alpha^2 + \beta^2}, \qquad x = (\alpha, \beta).$$

Atît f cît și g sînt compatibile cu relația R' definită la exemplul 3.

Propoziția 3.4. *Fie R o relație de echivalență pe o mulțime E și f o funcție oarecare de la E la F, compatibilă cu relația R. Atunci există o funcție $\bar{f}$ de la E/R la F, astfel încît $f = \bar{f} \circ \varphi$, φ fiind surjecția canonică de la E la E/R. Dacă f este surjectivă și dacă $f(x) = f(y)$ implică xRy, atunci $\bar{f}$ este bijectivă. Relația $f = \bar{f} \circ \varphi$ înseamnă că diagrama*



este comutativă.

Demonstrație. Se definește $\bar{f} : E/R \to F$ prin $\bar{f}(\hat{x}) = f(x)$, unde $\hat{x}$ este o clasă de echivalență iar x un repre-

Scanned with OKEN Scanner

zentant al acesteia. Funcţia f este bine definită. Într-adevăr dacă $y \in \hat{x}$ este un alt reprezentant al clasei $\hat{x}$, atunci xRy şi cum f este compatibilă cu R, rezultă $f(x) = f(y)$. Aşadar, $\bar{f}(\hat{x}) = \bar{f}(\hat{y})$ pentru $\hat{x} = \hat{y}$. Dacă $\varphi : E \to E/R$ este surjecţia canonică, este evident că $f = \bar{f} \circ \varphi$. Fie acum $g : E/R \to F$ o altă funcţie, astfel încît diagrama de mai sus să fie comutativă, adică $f = g \circ \varphi$. Atunci $g(\hat{x}) = g(\varphi(x)) = f(x)$. Prin urmare, $g = \bar{f}$ după definiţia lui $\bar{f}$, deci unicitatea este demonstrată. Restul rezultă uşor.

Corolarul 3.5. *Orice funcţie $f : E \to F$ poate fi descompusă sub forma $f = \bar{f} \circ \varphi$:*

$$E \xrightarrow{\varphi} E/R_f \xrightarrow{\bar{f}} F,$$

unde $\bar{f}$ este injectivă, iar φ este surjecţia canonică. (R_f este relaţia de echivalenţă asociată lui f.)

Demonstraţie. Avînd în vedere cele de mai înainte, rămîne de verificat doar că $\bar{f}$ este injectivă. Dacă $\bar{f}(\hat{x}) = \bar{f}(\hat{y})$, atunci $\bar{f}(\varphi(x)) = \bar{f}(\varphi(y))$, deci $f(x) = f(y)$. Dar aceasta înseamnă că $x \sim_R y$, de unde $\hat{x} = \hat{y}$, adică $\bar{f}$ este injectivă.

Din relaţia $f = \bar{f} \circ \varphi$ rezultă că $\bar{f}$ este surjectivă dacă şi numai dacă f este surjectivă. Aşadar, din propoziţia precedentă se obţine că $\bar{f}$ este bijectivă dacă şi numai dacă f este surjectivă.

Scanned with OKEN Scanner

CAPITOLUL II

Mulțimi de numere

§ 1. Construcția numerelor naturale

Încă din clasele elementare, elevii fac cunoștință cu mulțimea $\mathbb{N}$ a numerelor naturale

$$0,\ 1,\ 2,\ 3,\ldots,\ n,\ldots$$

acceptate în ultimă instanță ca obiecte matematice ce consemnează despre o mulțime, respectiv, proprietatea că :

— nu conține nici un element,

— conține un element și numai unul,

— conține un element și încă un element etc.

Numărul natural 1 este numit succesorul lui 0, 2 este numit succesorul lui 1, 3 este numit succesorul lui 2 etc.

Dacă se notează cu n' succesorul numărului natural n și cu s funcția $s : \mathbb{N} \to \mathbb{N}$ definită prin $s(n) = n'$, oricare ar fi $n \in \mathbb{N}$, numită *funcția succesor*, acceptăm ca plauzibile următoarele proprietăți ale numerelor naturale :

P_1) $s(n) \neq 0$ oricare ar fi $n \in \mathbb{N}$ (0 nu este succesorul unui număr natural).

P_2) s este funcție injectivă (numere naturale diferite au succesori diferiți)

Scanned with OKEN Scanner

P_3) Dacă M este o parte a lui $\mathbb{N}$, care conține 0 și odată cu orice n conține și pe $s(n)$, atunci $M = \mathbb{N}$ (căci M conține pe 0, $1 = s(0)$, $2 = s(1)$ ș.a.m.d.).

Matematicianul italian G. Peano (1858—1932), dînd statut de axiome proprietăților P_1), P_2) și P_3), a reușit să construiască cu ajutorul lor întreaga teorie a numerelor naturale. În principiu, teoria axiomatică a lui Peano folosește pentru numere modelul metodei logice, întrebuințat cu succes de Euclid în geometrie încă din antichitate.

În continuare se va lua ca bază definiția axiomatică a numerelor naturale dată de Peano. Conform acesteia, numerele naturale sînt elementele unei mulțimi $\mathbb{N}$ în care s-a fixat un element 0 (numit numărul natural 0) împreună cu o funcție $s : \mathbb{N} \to \mathbb{N}$ (numită funcție succesor) astfel încît axiomele P_1), P_2) și P_3) (numite axiomele lui Peano) să fie satisfăcute. Dacă $n \in \mathbb{N}$, atunci $s(n)$ se numește succesorul lui n și se notează, încă, cu n'. Succesorul lui 0 se notează cu 1, succesorul lui 1 se notează cu 2 ș.a.m.d., deci $s(0) = 1$, $s(1) = 2$ etc.

Observație. Axioma P_3) este la baza demonstrației prin inducție (primul principiu de inducție). Acesta poate fi formulat după cum urmează. Presupunem că fiecărui număr natural n i se asociază o propoziție $P(n)$. Fie $P(0)$ adevărată și dacă $P(k)$ este adevărată, atunci $P(s(k))$ este adevărată, atunci $P(n)$ este adevărată pentru orice $n \in \mathbb{N}$. Aceasta rezultă direct din axioma P_3). Fie M sumbulțimea lui $\mathbb{N}$, formată din numerele naturale k, pentru care $P(k)$ este adevărată. Atunci $0 \in M$ și dacă $m \in M$, atunci $s(m) \in M$. Prin urmare, după axioma P_3) $M = \mathbb{N}$ adică $P(n)$ este adevărată pentru toate numerele naturale.

Propoziția 1.1. *Cu notațiile precedente, rezultă* $s(\mathbb{N}) = \{n \in \mathbb{N} \mid n \neq 0\}$.

Demonstrație. Dacă punem $M = s(\mathbb{N}) \cup \{0\}$, atunci $M \subset \mathbb{N}$, $0 \in M$ și $s(M) \subset M$. Din P_3) rezultă $M = \mathbb{N}$ și cum $0 \notin s(M)$, se obține că orice număr natural nenul este succesorul unui număr natural.

Teorema 1.2 (*recursivă*). *Fie E o mulțime, φ o funcție de la E în ea însăși, x un element din E. Atunci există o unică funcție f de la $\mathbb{N}$ la E astfel încît*

$$f(0) = x, \quad f(s(n)) = \varphi(f(n)), \qquad n \in \mathbb{N}.$$

Scanned with OKEN Scanner

Demonstrație. Fie produsul cartezian $\mathbb{N} \times E$ și Γ mulțimea submulțimilor A ale lui $\mathbb{N} \times E$ cu următoarele proprietăți: 1° $(0, x) \in A$, 2° dacă $(n, y) \in A$, atunci $(s(n), \varphi(y)) \in A$. Evident, $\mathbb{N} \times E \in \Gamma$, deci $\Gamma \neq \emptyset$. Fie f intersecția tuturor submulțimilor A din Γ. Se va arăta că f este funcția de la $\mathbb{N}$ la E căutată. Mai întîi, prin inducție, rezultă că dacă $n \in \mathbb{N}$, există $y \in E$ astfel încît $(n, y) \in f$. Pentru a demonstra că f este o funcție, rămîne de arătat că dacă (n, y) și (n, y_1) aparțin lui f, atunci $y = y_1$. Pentru aceasta arătăm că submulțimea M a lui $\mathbb{N}$ formată din numerele $n \in \mathbb{N}$, cu proprietatea că dacă (n, y) și (n, y_1) aparțin lui f, atunci $y = y_1$, coincide cu $\mathbb{N}$. Procedăm prin inducție. Avem $0 \in M$, căci în caz contrar, există $(0, x)$, $(0, x_1) \in f$ cu $x \neq x_1$. Fie atunci f' submulțimea lui f, formată din toate elementele lui f mai puțin elementul $(0, x_1)$. Deci $f' \subsetneq f$. Pe de altă parte, f' satisface condițiile 1° și 2° își deci $f' \in \Gamma$. Așadar $f' \supset f$, ceea ce este absurd. Deci $0 \in M$. Fie un număr natural m, astfel încît $m \in M$, dar $s(m) \notin M$ și $(m, y) \in f$. Atunci $(s(m), \varphi(y)) \in f$ și cum $s(m) \notin M$, rezultă că există $z \neq \varphi(y)$ astfel că $(s(m), z) \in f$. Fie f'' submulțimea lui f formată din toate elementele lui f mai puțin elementul $(s(m), z)$ din f. Cum $s(m) \neq 0$ și $(0, x) \in f$, atunci $(0, x) \in f'$. Același argument arată că dacă $n \in \mathbb{N}$ și $n \neq m$, $(n, u) \in f'$, atunci $(s(n), \varphi(u)) \in f'$.

Acum dacă $(m, y_1) \in f'$, atunci $y = y_1$ și $(s(m), \varphi(y)) \in f'$ din modul cum a fost definit f'. Deci $f' \in \Gamma$ și atunci $f' \supset f$, ceea ce este în contradicție cu faptul că f' este submulțime proprie a lui f. Astfel, a rezultat că dacă $m \in M$, atunci $s(m) \in M$ și deci, din inducție, $M = \mathbb{N}$. Așadar, funcția f satisface cerințele. Pentru a demonstra unicitatea lui f, fie g o altă funcție care satisface aceleași condiții. Atunci $g \supset f$ și, după definiția funcției, este evident că $g = f$. Deci f este unică.

Cu ajutorul acestei teoreme recursive pot fi definite pe mulțimea $\mathbb{N}$ a numerelor naturale, două operații algebrice: adunarea și înmulțirea.

— *Adunarea numerelor naturale.* Fie $m, n \in \mathbb{N}$. *Suma* lui m și n (adică, m adunat cu n) poate fi definită luînd în teorema recursivă $x = m$ și φ aplicația succesor $n \to s(n)$

Scanned with OKEN Scanner

de la $\mathbb{N}$ la $\mathbb{N}$. Aşadar, după teorema recursivă, rezultă că pe mulţimea $\mathbb{N}$ a numerelor naturale există o operaţie algebrică (pe care o notăm aditiv) şi numai una, astfel încît:

1° $0 + m = m$, oricare ar fi $m \in \mathbb{N}$,
2° $s(n) + m = s(n + m)$, oricare ar fi $m, n \in \mathbb{N}$.

Lema 1.3. *Oricare ar fi* $m, n \in \mathbb{N}$, *atunci*:
1) $m + 0 = m$,
2) $m + s(n) = s(m + n)$.

Demonstraţie. Fie $M = \{m \in \mathbb{N} \mid m + 0 = m\}$. Cum $0 + 0 = 0$, atunci $0 \in M$. Dacă $m \in M$, atunci $s(m) + 0 = s(m + 0) = s(m)$ şi deci $s(m) \in M$. Aplicînd principiul inducţiei, rezultă $M = \mathbb{N}$ şi 1) este dovedită. Analog, se demonstrează 2).

Propoziţia 1.4. *Adunarea numerelor naturale este asociativă, comutativă şi admite pe 0 ca element neutru, adică*:
1) $(m + n) + p = m + (n + p)$,
2) $m + 0 = 0 + m = m$,
3) $m + n = n + m$,
oricare ar fi $m, n, p \in \mathbb{N}$.

Demonstraţie. 2) rezultă evident din cele de mai înainte. Pentru a demonstra 3), fie $m \in \mathbb{N}$ fixat şi $M = \{n \in \mathbb{N} \mid m + n = n + m\}$. Din 2) rezultă $0 \in M$. Dacă $n \in M$, după 2° şi 2) al lemei precedente se obţine

$$m + s(n) = s(m + n) = s(n + m) = s(n) + m$$

şi deci $s(n) \in M$. Aşadar, $M = \mathbb{N}$, ceea ce trebuia demonstrat. Restul lăsăm, ca exerciţiu, cititorului.

— *Înmulţirea numerelor naturale.* Pentru înmulţirea cu m, punem în teorema recursivă $n = 0$ şi φ aplicaţia $n \to n + m$. Aşadar, după teorema recursivă rezultă că pe mulţimea $\mathbb{N}$ a numerelor naturale există o operaţie algebrică (pe care o notăm multiplicativ), şi numai una, astfel încît:

1° $0m = 0$, oricare ar fi $m \in \mathbb{N}$,
2° $s(n)m = nm + m$, oricare ar fi $m, n \in \mathbb{N}$.

Scanned with OKEN Scanner

Lema 1.5. *Oricare ar fi* $m, n \in \mathbb{N}$, *atunci*:

1) $m0 = 0$,

2) $ms(n) = mn + n$.

Lăsăm demonstraţia ca exerciţiu, ea fiind analoagă aceleia de la lema 1.3.

Propoziţia 1.6. *Înmulţirea numerelor naturale este asociativă, comutativă şi admite pe* $1 = s(0)$ *ca element neutru, adică*:

1) $(mn)p = m(np)$.

2) $mn = nm$,

3) $1m = m1 = m$,

oricare ar fi $m, n, p \in \mathbb{N}$. *Mai mult, înmulţirea este distributivă faţă de adunare, adică*:

4) $m(n + p) = mn + mp$, *oricare ar fi* $m, n, p \in \mathbb{N}$.

Lăsăm demonstraţia, ca exerciţiu, ea fiind analoagă aceleia de la propoziţia 1.4.

— *Ordonarea numerelor naturale.* Pe mulţimea $\mathbb{N}$ a numerelor naturale se poate defini o relaţie de ordine $\leqslant$, numită *ordine naturală*, faţă de care $\mathbb{N}$ devine o mulţime bine ordonată.

Lema 1.7. *Dacă* m, n, p *sînt numere naturale, atunci următoarele afirmaţii sînt adevărate*:

1) $m + n = 0 \Rightarrow m = 0$ *şi* $n = 0$,

2) $m + n = m + p \Rightarrow n = p$,

3) $mn = 0 \Rightarrow m = 0$ *sau* $n = 0$,

4) $mn = 1 \Rightarrow m = n = 1$,

5) $mn = mp$ *şi* $m \neq 0 \Rightarrow n = p$.

Scanned with OKEN Scanner

Demonstrație. 1) Dacă $m \neq 0$, atunci $m = s(k)$, $k \in \mathbb{N}$. Deci $m + n = s(k) + n = s(k + n) \neq 0$. 2) Presupunem prin absurd, că $n \neq p$. Atunci, fie $M = \{m \in \mathbb{N} \mid m + n \neq m + p\}$. Cum $0 + n = n \neq p = 0 + p$, rezultă $0 \in M$. Dacă $m \in M$, atunci

$$s(m) + n = s(m + n) \neq s(m + p) = s(m) + p,$$

deci $s(m) \in M$. Din axioma P_3) a inducției avem $M = \mathbb{N}$, ceea ce contrazice ipoteza. 3) Dacă $m \neq 0$ și $n \neq 0$, atunci $m = s(k)$, $k \in \mathbb{N}$. Deci $mn = s(k)n = km + n \neq 0$, pentru că $n \neq 0$ (și se aplică 1)). Lăsăm cititorului, ca exercițiu, să demonstreze afirmațiile 4) și 5).

Relația binară $m < n$, care spune că *numărul natural m este mai mic decît numărul natural n*, poate fi definită, plecînd de la adunarea numerelor naturale:

$$m < n \Leftrightarrow \text{există } u \in \mathbb{N}, u \neq 0, \text{ astfel încît } n = m + u.$$

(După regula de simplificare pentru adunare, un astfel de element u, dacă există, este unic).

De obicei, se scrie:

$$m \leqslant n \text{ dacă } m < n \text{ sau } m = n$$

($m \leqslant n$ se citește „*m mai mic sau egal cu n*").

$$n > m \text{ dacă } m < n$$

($n > m$ se citește „*n mai mare ca m*").

Observație. Din aceste definiții se deduc proprietățile obișnuite ale inegalităților. De exemplu, regula de tranzitivitate afirmă că dacă $k < m$ și $m < n$, atunci $k < n$.

Pentru a o demonstra, fie $k + u = m$ și $m + v = n$ ($u, v \in \mathbb{N}$; $u, v \neq 0$); atunci $k + (u + v) = n$. Mai mult, $u + v \neq 0$ și deci $k < n$.

Propoziția 1.8 (*regula de tricotomie*). *Pentru orice două numere naturale m și n una din următoarele relații și numai una este adevărată:*

$$m < n, \qquad m = n, \qquad m > n.$$

Scanned with OKEN Scanner

Demonstrație. După lema 1.7 se arată, fără dificultate, că relațiile de mai sus se exclud două cîte două. De exemplu, dacă în același timp $m < n$ și $m = n$, atunci $n = m + u$, $u \neq 0$; dar regula de simplificare dă $u = 0$ (contradicție). Relațiile $m < n$ și $m > n$ conduc la o contradicție de același gen. Rămîne să demonstrăm că cel puțin una din relații este adevărată. Se procedează prin inducție, după n, pentru fiecare m.

Pentru $n = 0$, este clar, deoarece m este sau egal cu 0, sau diferit de 0 (adică > 0). Presupunem deci că alternativa este adevărată pentru orice $m \in \mathbb{N}$ și pentru un anumit n și să arătăm că, pentru orice $k \in \mathbb{N}$, una din relațiile

$$k < s(n), \quad k = s(n), \quad k > s(n)$$

este adevărată. Dacă $k = 0$, prima este adevărată. Dacă nu, $k \neq 0$ și $k = s(m)$ pentru un $m \in \mathbb{N}$. După ipoteza de inducție una din relațiile $m > n$, $m = n$ sau $m < n$ este adevărată. Aplicînd s la ambii membri ai acestor inegalități, se obțin cele trei relații.

Iată alte proprietăți ale relației de ordine, legate de adunarea și înmulțirea numerelor naturale.

Propoziția 1.9 *Fie m, n, p numere naturale. Atunci următoarele afirmații sînt adevărate:*

1) *dacă $m < n$, atunci $m + p < n + p$;*

2) *dacă $m < n$ și $p \neq 0$, atunci $mp < np$.*

Demonstrație. 1) Fie $u \neq 0$, astfel încît $m + u = n$. Atunci $m + p + u = n + p$ cu $u \neq 0$ și deci $m + p < n + p$.

2) De asemenea, din $m + u = n$ rezultă $(m + u)p = np$, de unde $mp + up = np$. Dar din lema 1.7, 3), rezultă $up \neq 0$ și deci $mp < np$.

Propoziția 1.10 ($\mathbb{N}$ *este bine ordonată*). *Orice mulțime nevidă A de numere naturale are un prim element, adică un element $a \in A$ astfel încît $a \leqslant x$ pentru orice $x \in A$.*

Scanned with OKEN Scanner

Demonstrație. Dacă $0 \in A$, atunci 0 este primul element al său. Dacă $0 \notin A$, fie M mulțimea numerelor naturale n, astfel încît $n \leqslant x$, oricare ar fi $x \in A$. Evident, $0 \in M$ și dacă $x \in A$, atunci $s(x) \notin M$. Deci $M \neq \mathbb{N}$ și, după axioma inducției, există un număr natural $a \in M$ astfel încît $s(a) \notin M$ (în caz contrar, ar rezulta $M = \mathbb{N}$). Atunci a este numărul căutat, deoarece $a \leqslant x$, pentru orice $x \in A$. Mai mult, $a \in A$, căci altfel $a < x$ pentru orice $x \in A$ și deci $s(a) \leqslant x$, pentru orice $x \in A$. Deci $s(a) \in M$ (contradicție !).

Observație. Proprietatea mulțimii numerelor naturale de a fi bine ordonată stă la baza celui de-al doilea principiu de inducție, care ne dă o nouă metodă de demonstrație prin inducție. Dăm o aplicație a acestuia.

Corolarul 1.11. *Nu există nici un număr natural între* 0 *și* 1.

Demonstrație. Presupunem, prin absurd, că există un număr natural k astfel încît $0 < k < 1$. Mulțimea A a numerelor naturale cu această proprietate este deci nevidă și după propoziția precedentă are un prim element a, astfel că $0 < a < 1$. Multiplicînd cu a și ținînd seama de propoziția 1.9, se obține $0 < aa < a$, ceea ce contrazice faptul că a este primul element al lui A. Această contradicție demonstrează corolarul.

Al doilea principiu de inducție matematică este conținut în teorema următoare.

Teorema 1.12. *Dacă o mulțime* $B \subset \mathbb{N}$ *are pentru orice* $n \in \mathbb{N}$ *proprietatea*

$$n \in B \text{ dacă, pentru orice } m \in \mathbb{N},\ m < n \Rightarrow m \in B,$$

atunci $B = \mathbb{N}$.

Demonstrație. Fie că $B \neq \mathbb{N}$. După propoziția 1.10 există un prim număr natural b care nu aparține lui B. Pentru că b este primul, orice $m < b$ aparține lui B. Rezultă după ipoteză că $b \in B$, ceea ce este în contradicție cu faptul că $b \notin B$. Deci $B = \mathbb{N}$.

Scanned with OKEN Scanner

Lema 1.13 (*Arhimede*). *Dacă* $m, n \in \mathbb{N}$, $n \neq 0$, *atunci există* $k \in \mathbb{N}$, *astfel încît* $kn > m$.

Demonstrație. Mai întîi, rezultă $mn \geqslant m$. Într-adevăr, dacă $m = 0$ sau $n = 1$, atunci $mn = m$. Fie acum $m \neq 0$, $n \neq 1$. Deci $n = s(l)$, $l \neq 0$. Cum $n = l + 1$, rezultă $mn = m(l + 1) = ml + m > m$, deoarece $ml > 0$. Fie $k = m + 1$ și se obține

$$kn = (m + 1)n = mn + n > mn \geqslant m,$$

de unde $kn > m$.

Teorema 1.14 (*teorema împărțirii cu rest*). *Dacă* $m, n \in \mathbb{N}$ *și* $n \neq 0$, *atunci există* q, $r \in \mathbb{N}$, *unic determinați, astfel încît*

$$m = nq + r, \qquad r < n.$$

Demonstrație. Fie A mulțimea numerelor naturale de forma nk, astfel încît $nk > m$. Datorită lemei lui Arhimede, mulțimea A este nevidă și fie nl primul element al acestei mulțimi. Evident $l \neq 0$, deoarece altfel $n0 = 0 > m$, ceea ce este absurd. Fie atunci $q \in \mathbb{N}$, astfel încît $l = s(q) = q + 1$. Cum $nq < n(q + 1) = nl$, rezultă $nq \leqslant m$, căci altfel nl n-ar mai fi primul element al lui A. Fie atunci $r \in \mathbb{N}$ astfel încît $m = nq + r$. Dacă $n \leqslant r$, atunci $n + u = r$ cu $u \in \mathbb{N}$. Deci $m = nq + r = nq + n + u = n(q + 1) + u = nl + u$, de unde $nl \leqslant m$, ceea ce este absurd. Așadar $r < n$. Rămîne de verificat unicitatea lui q și r. Fie pentru aceasta $q_1, r_1 \in \mathbb{N}$ două numere naturale, astfel încît

$$m = nq_1 + r_1 \quad \text{cu } r_1 < n$$

și să arătăm că $q = q_1$ și $r = r_1$. Dacă $q \neq q_1$, atunci $q < q_1$ sau $q_1 < q$. Dacă $q < q_1$, atunci există $u \in \mathbb{N}$, $u \neq 0$, astfel încît $q + u = q_1$. Atunci $nq_1 + r_1 = n(q + u) + r_1 = nq + nu + r_1$, deci $nq + r = nq + nu + r_1$, de unde $r = nu + r_1 \geqslant nu + n$, ceea ce este absurd. La fel se arată că nu este posibil ca $q_1 < q$. Deci $q = q_1$ și de aici rezultă imediat $r = r_1$.

Scanned with OKEN Scanner

Dacă m este un număr natural, atunci numerele $0m = 0$, $1m = m$, $2m = m + m, \ldots, km$, $(k + 1)m = km + m, \ldots$ se numesc *multiplii lui* m.

Fie m şi n două numere naturale. Se spune că m divide n dacă n este egal cu un multiplu al lui m şi notăm $m|n$ (se citeşte „m divide n"). Aşadar, $m|n \Leftrightarrow$ există $u \in \mathbb{N}$ astfel încît $n = um$.

Dacă $m|n$, se spune încă că *n este un multiplu de m* sau că *n se divide prin m*.

Din egalităţile $0m = 0$ şi $1m = m$ rezultă că $m|0$, respectiv $1|m$ şi $m|m$, oricare ar fi $m \in \mathbb{N}$. Dacă $m \neq 0$, atunci relaţia $m|n$ este echivalentă cu faptul că restul împărţirii lui n prin m este egal cu 0.

Fie pe $\mathbb{N}$ relaţia binară D, $D \subset \mathbb{N} \times \mathbb{N}$, definită astfel :

$$(m, n) \in D \Leftrightarrow m|n$$

şi numită *relaţia de divizibilitate* pe $\mathbb{N}$.

Propoziţia 2.1. *Relaţia de divizibilitate pe $\mathbb{N}$ este reflexivă, antisimetrică şi tranzitivă. Cu alte cuvinte, avem :*

1) $m|m$, *oricare ar fi* $m \in \mathbb{N}$;

2) *dacă* $m|n$ *şi* $n|m$, *atunci* $m = n$;

3) *dacă* $m|n$ *şi* $n|p$, *atunci* $m|p$.

Demonstraţie. Reflexivitatea relaţiei de divizibilitate rezultă din egalitatea $1m=m$ valabilă pentru orice număr natural m. 2) Dacă $m|n$ şi $n|m$, atunci $n = um$ şi $m = vn$ cu u şi v numere naturale, de unde $m = vum$. Dacă $m = 0$, atunci $n = 0$, deci $m = n$. Dacă $m \neq 0$, atunci din $1m = vum$ rezultă $1 = vu$ şi, acum, după lema 1.7 rezultă $u = v = 1$, deci $m = n$. Aşadar, relaţia de divizibilitate este antisimetrică. 3) Dacă $m|n$ şi $n|p$, atunci $n = um$ şi $p = vn$ cu $u, v \in \mathbb{N}$. Rezultă $p = (vu)n$, deci $m|p$.

Deci, relaţia de divizibilitate pe $\mathbb{N}$ este o relaţie de ordine.

Scanned with OKEN Scanner

Definiția 2.1. Un număr natural $p > 1$ se numește *prim* dacă oricare ar fi m, n numere naturale, $p \mid mn \Rightarrow p \mid m$ sau $p \mid n$.

Un număr natural $b > 1$ se numește *indecompozabil* dacă din

$$u \mid b \Rightarrow u = 1 \text{ sau } u = b.$$

Un număr natural $m > 1$ care nu este indecompozabil se numește *decompozabil*.

Lema 2.2. *Fie m și n două numere naturale astfel încît $m \mid n$ și $n \neq 0$. Atunci $m \leqslant n$.*

Demonstrație. Fie $u \in \mathbb{N}$ astfel încît $um = n$. Cum $n \neq 0$, rezultă $u \neq 0$, deci $u = v + 1$ cu $v \in \mathbb{N}$. Dar

$$n = mu = m(v + 1) = mv + m,$$

de unde $m \leqslant n$.

Lema 2.3. *Fie m, n, p trei numere naturale, astfel încît $m = n + p$. Dacă numărul natural q divide oricare două dintre numerele m, n, p atunci q divide și pe al treilea.*

Demonstrație. Fie $q \mid n$ și $q \mid p$. Atunci $n = uq$ și $p = vq$ cu $u, v \in \mathbb{N}$. Rezultă $m = (u + v)q$, deci $q \mid m$. Fie $q \mid m$ și $q \mid n$. Atunci $m = uq$ și $n = vq$ cu $u, v \in \mathbb{N}$. Din $uq = vq + p$ rezultă $uq \geqslant vq$, deci $u \geqslant v$, de unde $u = v + w$ cu $w \in \mathbb{N}$. Acum din $uq = vq + p$ rezultă $vq + wq = vq + p$, deci $wq = p$, de unde $q \mid p$. Analog, se arată că din $q \mid m$ și $q \mid p$ rezultă $q \mid n$.

Lema 2.4. *Fie m un număr natural > 1. Următoarele afirmații sînt echivalente:*

1) *m este decompozabil;*

2) *există $n, p \in \mathbb{N}$, astfel încît $m = np$; cu $1 < n < m$ și $1 < p < m$.*

Demonstrație. 1) $\Rightarrow$ 2). Cum m este decompozabil, rezultă că admite un divizor n diferit de 1 și m. Fie p,

Scanned with OKEN Scanner

astfel încît $m = np$. Cum $m \neq 0$, din lema 2.2 rezultă $1 \leqslant n \leqslant m$ și cum n este diferit de 1 și m, se deduce $1 < n < m$. La fel $1 \leqslant p \leqslant m$. Dacă $p = 1$, atunci $m = n$ iar dacă $p = m$, atunci $n = 1$. În ambele cazuri se obține o contradicție, deci $1 < p < m$.

Lema 2.5. *Orice număr natural $m > 1$ admite un divizor indecompozabil.*

Demonstrație. Mulțimea $P = \{q \in \mathbb{N} \mid q \text{ divide } m, q > 1\}$ nu este vidă, căci conține pe m. Cum $\mathbb{N}$ este bine ordonată, fie b cel mai mic număr din P. Evident $b > 1$. Dacă b este decompozabil, există $n, p \in \mathbb{N}$, astfel încît

$$b = np, \qquad 1 < n < b \text{ și } 1 < p < b$$

(vezi lema 2.4). Dar, din $n \mid b$ și $b \mid m$ rezultă $n \mid m$ și cum $n > 1$, rezultă $n \in P$. Dar $n < b$ și $n \in P$ contrazice alegerea lui b. Rămîne deci adevărat că b este indecompozabil și evident este divizor al lui m.

Teorema 2.6. *Fie p un număr natural > 1. Următoarele afirmații sînt echivalente:*

1) *p este prim;*
2) *p este indecompozabil.*

Demonstrație. 1) $\Rightarrow$ 2). Fie k un divizor al lui p. Există $l \in \mathbb{N}$ astfel încît $kl = p$. Din $1 \cdot p = kl$ rezultă că $p \mid kl$. Cum p este prim, rezultă $p \mid k$ sau $p \mid l$. Dacă $p \mid k$, atunci $k = pu$ cu $u \in \mathbb{N}$. Din $p = kl$ rezultă $p = pul$, deci $l = ul$. Din lema 1.7 rezultă $u = l = 1$ și deci $k = p$. La fel, dacă $p \mid l$ deducem $k = 1$. Așadar, p este indecompozabil.

2) $\Rightarrow$ 1). Presupunem că există elemente indecompozabile care nu sînt prime. Fie p cel mai mic element indecompozabil care nu este prim ($\mathbb{N}$ este bine ordonată). Cum p nu este prim, există $m, n \in \mathbb{N}$ astfel încît $p \mid mn$ și p nu

Scanned with OKEN Scanner

divide pe m și nici pe n. Dar $m > 1$, deoarece $m = 0$ implică $p \mid m$, iar $m = 1$ și $p \mid mn$ implică $p \mid n$. La fel, rezultă $n > 1$. Putem încă presupune că $m < p$ și $n < p$.

Într-adevăr, dacă $m > p$, atunci $m = pq + r$ cu $0 < r < p$ și din egalitatea

$$mn = pqn + rn$$

rezultă că $p \mid rn$ (vezi lema 2.3) și evident p nu divide pe r. Deci se poate înlocui m cu r. La fel se procedează dacă $n > p$. Mai mult, se pot alege m și n astfel încît produsul mn să fie minim (deoarece $\mathbb{N}$ este bine ordonată). Cum $p \mid mn$, există $q \in \mathbb{N}$ astfel încît $mn = pq$. Rezultă $q > 1$, căci $q = 1$ implică $m \mid p$ și $n \neq p$ și cum p este indecompozabil, rezultă $m = p$ sau $n = p$ (contradicție !). Fie b un divizor indecompozabil al lui q (vezi lema 2.5). Avem

$$pq = mn < pp$$

De aici, rezultă $q < p$, așadar $b \leqslant q < p$. Cum $b \mid q$ și $q \mid mn$, rezultă că $b \mid mn$. Dar b este prim (căci p este cel mai mic număr indecompozabil care nu este prim). Rezultă că $b \mid m$ sau $b \mid n$. Presupunem că $b \mid m$. Fie $m_1, q_1 \in \mathbb{N}$ astfel încît $m = bm_1$ și $q = bq_1$ Din $mn = qp$ rezultă $b\, m_1 n = b\, q_1 p$, deci $m_1 n = q_1 p$. Așadar, $p \mid m_1 n$ și evident p nu divide nici pe m_1 și nici pe n. Cum $b > 1$, rezultă $m_1 < m$ și deci $m_1 n < mn$ (contradicție !).

Lema 2.7. *Orice număr natural > 1 este sau prim sau produs de numere prime.*

Demonstrație. Fie M mulțimea ce cuprinde pe 0 și 1 și toate numerele naturale > 1 care sînt prime sau produs de prime. Dacă M conține toate numerele întregi $m \leqslant n$, atunci M conține și pe $n + 1$. Într-adevăr, dacă $n + 1$ este prim, atunci conform definiției lui M rezultă $n + 1 \in M$. Dacă $n + 1$ nu este prim, atunci după teorema 2.6 rezultă $n + 1 = km$, cu $1 < k < n + 1$ și $1 < m < n + 1$. Deci k și m sînt din M și atunci ele sînt numere prime sau produs

Scanned with OKEN Scanner

de numere prime, de unde $n+1=km$ este un produs de numere prime. Aşadar, $n+1 \in M$. După axioma inducţiei rezultă $M=\mathbb{N}$, de unde se obţine rezultatul din enunţ.

Teorema 2.8 (*fundamentală a aritmeticii*). *Orice număr natural* $n>1$ *poate fi descompus în mod unic* (*abstracţie făcînd de ordinea factorilor*) *în produs de numere prime*:

$$n=p_1p_2\ldots p_k \qquad (k\geqslant 1).$$

Demonstraţie. În lema precedentă s-a demonstrat că există cel puţin o astfel de descompunere. Mai rămîne de arătat unicitatea. Cu alte cuvinte, dacă

$$n=p_1p_2\ldots p_k=q_1q_2\ldots q_l \qquad (2.1)$$

sînt două descompuneri în factori primi ale lui n, atunci $k=l$ şi dacă facem eventual o renumerotare a factorilor, atunci $p_i=q_i$, $i=1, 2,\ldots,k$.

Din egalitatea (2.1) se obţine

$$p_1 \mid q_1q_2\ldots q_l$$

şi cum p_1 este prim, rezultă că p_1 divide cel puţin unul dintre numerele $q_1, q_2,\ldots, q_l$. Pentru comoditate să presupunem că p_1 divide pe q_1 (pentru a le aranja astfel, putem, eventual, face o renumerotare a numerelor $q_1, q_2,\ldots q_l$). Cum $p_1 \mid q_1$, rezultă $1<p_1\leqslant q_1$ şi cum q_1 este prim, după teorema 2.6 avem $p_1=q_1$. Simplificînd în (2.1) cu $p_1=q_1$, se obţine

$$m=p_2\ldots p_k=q_2\ldots q_l.$$

Vom proceda prin inducţie şi anume presupunem că proprietatea este adevărată pentru toate numerele naturale $m<n$. Astfel, numerele $p_2,\ldots,p_k$ coincid, exceptînd ordinea, cu numerele $q_2,\ldots,q_l$ şi deci acelaşi lucru este adevărat şi pentru $p_1, p_2,\ldots, p_k$ şi $q_1, q_2,\ldots,q_l$. De aici rezultă unicitatea descompunerii în factori primi pentru n.

Corolarul 2.9 (*Euclid*). *Există o infinitate de numere naturale prime.*

Demonstraţie. Să presupunem, prin absurd, că există doar un număr finit de astfel de numere şi fie q cel mai mare dintre acestea. Considerăm numărul $n=q!+1$

Scanned with OKEN Scanner

și fie p un divizor prim al său. Deci $p \mid q! + 1$, dar evident $p \mid q!$, de unde $p \mid 1$ și $p \leqslant 1$, adică se obține o contradicție.

Observație. Teorema 2.8 constituie punctul de plecare în studiul teoriei numerelor. În cap. IV va fi dată o generalizare a acesteia pentru inelele cu descompunere unică în factori primi.

§ 3. Construcția numerelor întregi

În acest paragraf vom arăta cum poate fi construită mulțimea $\mathbb{Z}$ a numerelor întregi, plecînd de la mulțimea $\mathbb{N}$ a numerelor naturale. Proprietățile adunării și înmulțirii în $\mathbb{Z}$ vor fi, grație acestei construcții, deduse din acelea ale lui $\mathbb{N}$.

În $\mathbb{N}$ ecuația $m + x = n$, în care m și n sînt numere naturale, nu are neapărat o soluție în $\mathbb{N}$. O astfel de ecuație are o soluție în $\mathbb{N}$ dacă și numai dacă $m \geqslant n$. În acest caz, evident, soluția este unică.

Deci dacă $m, n \in \mathbb{N}$, $m \geqslant n$, există $x \in \mathbb{N}$ unic, astfel încît $m + x = n$. Numărul x se numește *diferența* dintre m și n, iar legea prin care se asociază perechii de numere (m, n) elementul x se numește *scădere*.

Așadar, în $\mathbb{N}$ scăderea nu este întotdeauna posibilă (nu este operație algebrică pe $\mathbb{N}$).

Pentru a face posibilă întotdeauna scăderea, mulțimea $\mathbb{N}$ va fi extinsă la o mulțime mai cuprinzătoare care va constitui mulțimea $\mathbb{Z}$ a numerelor întregi. Se vor adăuga noi elemente la mulțimea numerelor naturale, astfel încît noua mulțime să satisfacă cerința impusă. $\mathbb{Z}$ este mulțimea

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Mai formal, $\mathbb{Z}$ se poate concepe în modul următor: $\mathbb{N}$ fiind mulțimea numerelor naturale și $\mathbb{N}^*$ mulțimea numerelor naturale nenule, se consideră mulțimea $\{-\}$ formată dintr-un singur element „$-$”. În produsul cartezian $\{-\} \times \mathbb{N}^*$ cuplul $(-, n)$ se va scrie simplu $-n$. Mulțimile $\{-\} \times \mathbb{N}^*$ și $\mathbb{N}$ sînt disjuncte. Fie $\mathbb{Z}$ reuniunea (disjunctă)

Scanned with OKEN Scanner

a lor. Acesta ne arată că orice element a din $\mathbb{Z}$ este fie un număr natural, fie „opusul" (formal) $-n$ al unui număr natural.

În continuare, se vor nota cu $a, b, c, \ldots$ elementele mulțimii $\mathbb{Z}$ și cu $k, m, n, p, \ldots$ elementele mulțimii $\mathbb{N}$.

Ne propunem să construim o mulțime $\mathbb{Z}$ care să conțină mulțimea $\mathbb{N}$ a numerelor naturale și pe care să o înzestrăm cu două operații algebrice (adunarea și înmulțirea), astfel încît : în $\mathbb{Z}$ să fie posibilă scăderea, adunarea în $\mathbb{Z}$ să fie obținută prin prelungirea adunării date în $\mathbb{N}$ și, în sfîrșit, toate noile elemente adăugate la $\mathbb{N}$ să fie necesare pentru a face posibilă scăderea.

Pentru a realiza acest lucru, se procedează în modul următor. Fie produsul cartezian $\mathbb{N} \times \mathbb{N}$, adică mulțimea

$$\mathbb{N} \times \mathbb{N} = \{(m, n) \mid m, n \in \mathbb{N}\}.$$

Pe această mulțime se definește relația binară $\sim$ astfel :

$$(m, n) \sim (m', n') \Leftrightarrow m + n' = m' + n.$$

Aceasta este o relație de echivalență, adică : reflexivă, simetrică și tranzitivă.

Să demonstrăm, de exemplu, tranzitivitatea relației, adică dacă $(m, n) \sim (m', n')$ și $(m', n') \sim (m'', n'')$, atunci $(m, n) \sim (m'', n'')$. Într-adevăr, din $m + n' = m' + n$ și $m' + n'' = m'' + n'$ rezultă adunînd membru cu membru aceste două egalități :

$$m + n' + m' + n'' = m' + n + m'' + n'$$

și deci

$$m + n'' = m'' + n.$$

Această relație de echivalență împarte mulțimea $\mathbb{N} \times \mathbb{N}$ în clase de echivalență.

Definiția 3.1. Fiecare clasă de echivalență din mulțimea factor $\mathbb{N} \times \mathbb{N}/\sim$ se numește *număr întreg*. Mulțimea numerelor întregi se notează cu $\mathbb{Z}$.

Scanned with OKEN Scanner

Fie $(\overline{m, n})$ clasa de echivalenţă a perechii (m, n).

Pe scurt, două perechi de numere naturale (m, n) şi (m', n') sînt reprezentanţi ai aceluiaşi număr întreg, dacă şi numai dacă $m + n' = m' + n$.

Propoziţia 3.1. *Orice reprezentant al numărului întreg* $(\overline{m, n})$ *se obţine adăugînd sau scăzînd (dacă este posibil) din cele două componente ale perechii* (m, n) *acelaşi număr natural.*

Demonstraţie. Fie $(\overline{m, n}) = (\overline{m', n'})$, adică $m + n' = m' + n$. Prespunem, de exemplu, că $m' \geqslant m$. Atunci există un număr natural p astfel încît $m' = m + p$. Se poate scrie succesiv $m + n' = m' + n$, sau $m + n' = m + p + n$ şi deci $n' = m + p$. Astfel sînt verificate, simultan, relaţiile

$$m' = m + p \quad \text{şi} \quad n' = n + p.$$

Reciproc, fie perechile (m, n) şi $(m + p, n + p)$. Din $m + (n + p) = (m + p) + n$ rezultă $(m, n) \sim (m + p, n + p)$, adică $(\overline{m, n}) = (\overline{m + p, n + p})$.

În continuare, se vor căuta reprezentanţi cît mai convenabili pentru numerele întregi. Fie, aşadar, $(\overline{m, n})$ un număr întreg, perechea (m, n) fiind un reprezentant al său. Se disting următoarele trei cazuri:

1° $m > n$. Atunci există un număr natural p, astfel încît $m = n + p$. Se poate scrie $(m, n) = (n + p, n)$ şi scăzînd din ambele componente pe n, rezultă $(m, n) \sim (p, 0)$. În acest caz, se spune că numărul întreg $(\overline{m, n}) = (\overline{p, 0})$ este *pozitiv* şi se notează, de asemenea, cu $+p$.

2° $m = n$. Scăzînd din ambele componente ale perechii (m, n) pe $m = n$, se obţine $(m, n) \sim (0, 0)$. În acest caz, se spune că numărul întreg este *nul* şi se notează cu 0; se mai numeşte şi *numărul zero*.

3° $m < n$. Există atunci un număr natural q, astfel încît $n = m + q$. Se poate deci scrie $(m, n) = (m, m + q)$

Scanned with OKEN Scanner

și scăzînd din ambele componente pe m, se obține $(m, n) \sim$ $\sim (0, q)$. În acest caz, se spun că numărul întreg $(\overline{m, n}) =$ $= (\overline{0, q})$ este *negativ* și se notează cu $-q$.

Observăm că pentru orice număr întreg există un unic reprezentant al său care să aibă cel puțin una din componente egală cu 0. Așadar, mulțimea $\mathbb{Z}$ se scrie

$$\mathbb{Z} = \{\ldots, (\overline{0, n}), \ldots, (\overline{0, 2}), (\overline{0, 1}), (\overline{0, 0}), (\overline{1, 0}), (\overline{2, 0}), \ldots \ldots, (\overline{n, 0}), \ldots\}.$$

Dacă $(\overline{m, n})$ este un număr întreg, atunci reprezentantul său care are cel puțin una din componente nulă se numește *reprezentant canonic* al numărului întreg $(\overline{m, n})$. Cealaltă componentă a reprezentantului canonic se numește *valoare absolută* (sau *modul*) a numărului considerat și se notează $|(\overline{m, n})|$. Vom reveni spre sfîrșitul paragrafului cu cîteva proprietăți ale valorii absolute.

În concluzie, un număr întreg nenul poate fi reprezentat printr-un număr natural (valoarea sa absolută) precedat de un semn (+ dacă numărul este pozitiv, — dacă numărul este negativ). Numărul 0 are valoarea absolută 0; i se poate atibui, după voie, semnul + sau semnul —, semn care se omite, în general.

Deci:

$$\mathbb{Z} = \{\ldots, -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, \ldots\}.$$

Observație. Convenim să identificăm numărul întreg pozitiv (sau nul) $+p$ cu numărul natural p. Fiecare număr întreg, pozitiv sau nul este considerat deci, prin această convenție, egal cu valoarea sa absolută. Se va justifica această convenție, în continuare. Mai precis, se va vedea că orice definiție referitoare la numerele întregi este în concordanță, cînd este vorba de numere pozitive, cu definiția corespunzătoare de la numerele naturale.

Vom da acum o reprezentare grafică (vezi fig. 1) a mulțimii numerelor întregi în care să punem în evidență perechile de numere naturale ce reprezintă același număr

Scanned with OKEN Scanner

întreg. Considerăm două axe de coordonate perpendiculare. Fiecare pereche (m, n) de numere naturale are ca imagine un punct (în primul cadran) de abscisă m și ordonată n. Toate perechile care dau același număr întreg (adică echivalente între ele) au imaginile situate pe o paralelă la prima bisectoare. Ele dau același număr întreg care apare scris pe axa ordonatelor, la intersecția sa cu direcția considerată.

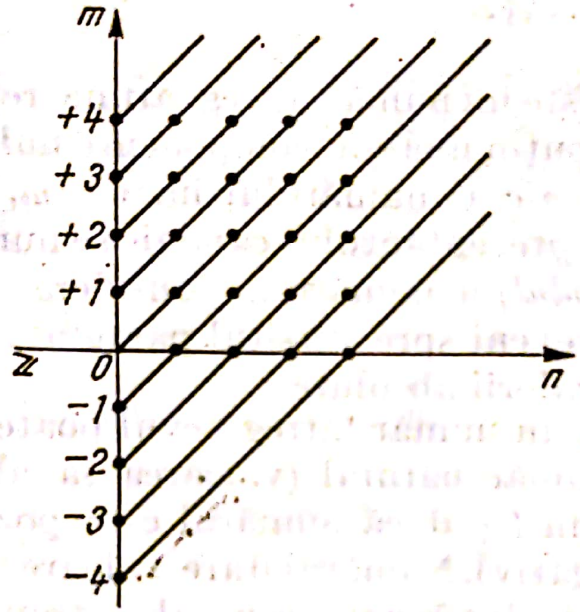


Fig. 1

— *Adunarea numerelor întregi.* Pe mulțimea $\mathbb{Z}$ a numerelor întregi se va defini o operație algebrică care se numește *adunare* și care se notează cu același simbol $+$ ca și la numerele naturale.

Dacă $(\overline{m, n})$ și $(\overline{m', n'})$ sînt două numere întregi, se pune

$$\overline{(m, n)} + \overline{(m', n')} = (\overline{m + m'}, \overline{n + n})'.$$

Numărul întreg $(\overline{m+m', n+n'})$ se numește *suma* numerelor întregi $(\overline{m, n})$ și $(\overline{m', n'})$, iar operația prin care celor două numere întregi $(\overline{m, n})$ și $(\overline{m', n'})$ li se asociază suma lor se numește *adunare*. Trebuie demonstrat că operația de adunare a numerelor întregi este bine definită, în sensul

că dacă se schimbă reprezentanții numerelor care se adună, se obține același număr ca sumă. Cu alte cuvinte, dacă

$$(m, n) \sim (m_1, n_1) \text{ și } (m', n') \sim (m'_1, n'_1),$$

atunci

$$\overline{(m + m', n + n')} = \overline{(m_1 + n'_1, n_1 + n'_1)}.$$

Într-adevăr, rezultă $m + n_1 = m_1 + n$ și $m' + n'_1 = m'_1 + n'$ care, adunate membru cu membru, dau succesive:

$$(m + m') + (n_1 + n'_1) = (m_1 + m'_1) + (n + n'_1),$$

adică

$$(m + m', n + n'_1) \sim (m_1 + m'_1, n_1 + n'_1).$$

Fie reprezentanți canonici ai numerelor întregi.

1° Adunarea a două numere întregi pozitive:

$$\overline{(p, 0)} + \overline{(p', 0)} = \overline{(p + p', 0)},$$

ceea ce se scrie de asemenea

$$(+p) + (+p') = +(p + p').$$

2° Adunarea a două numere întregi negative:

$$\overline{(0, q)} + \overline{(0, q')} = \overline{(0, q + q')},$$

ceea ce se scrie de asemenea

$$(-q) + (-q') = -(q + q').$$

3° Adunarea a două numere întregi, unul pozitiv, altul negativ:

$$\overline{(p, 0)} + \overline{(0, q)} = \overline{(p, q)}.$$

Să găsim reprezentantul canonic al sumei $\overline{(p, q)}$. Dacă $p \geqslant q$, există $k \in \mathbb{N}$ astfel încît $p = k + q$ și deci

$$\overline{(p, q)} = \overline{(k + q, q)} = \overline{(r, 0)},$$

ceea ce se scrie de asemenea

$$p + (-q) = r.$$

Dacă $p \leqslant q$, există $r \in \mathbb{N}$ astfel încît $q = r + p$ și deci

$$(\overline{p,\ q}) = (\overline{p,\ r+q}) = (\overline{0,\ r}),$$

ceea ce se scrie de asemenea

$$p + (-q) = -r.$$

Teorema 3.2. *Adunarea numerelor întregi are proprietățile :*

1) $a + a' = a' + a$, *oricare ar fi* $a, a' \in \mathbb{Z}$ (*comutativitate*);

2) $a + (a' + a'') = (a + a') + a''$, *oricare ar fi* $a, a', a'' \in \mathbb{Z}$ (*asociativitate*);

3) $a + 0 = 0 + a = a$, *oricare ar fi* $a \in \mathbb{Z}$ (0 este *element neutru*);

4) *oricare ar fi* $a \in \mathbb{Z}$, *există* $a^* \in \mathbb{Z}$, *astfel încît*

$$a + a^* = a^* + a = 0.$$

Demonstrație. 1) Fie $a = (\overline{m, n})$, $a' = (\overline{m', n'})$ numere întregi. Atunci $a + a' = (\overline{m, n}) + (\overline{m', n'}) = (\overline{m + m', n + n'}) = (\overline{m' + m, n' + n}) = (\overline{m', n'}) + (\overline{m, n}) = a' + a$.

2) Asociativitatea se demonstrează analog, folosind asociativitatea adunării numerelor naturale.

3) Dacă $a = (\overline{m, n})$, atunci $n + 0 = (\overline{m, n}) + (0, 0) = (\overline{m, n}) = a$.

4) Dacă $a = (\overline{m, n})$, atunci $a^* = (\overline{n, m})$ are proprietatea cerută, adică $a + a^* = |(\overline{m,\ n})| + (\overline{n,\ m}) = (\overline{m + n,\ m + n}) = 0$.

Numărul a^* se numește *opusul* lui a.

Considerînd reprezentanți canonici ai numerelor întregi, se poate scrie, de exemplu :

$$(\overline{p, 0}) + (\overline{0, p}) = p + (-p) = 0.$$

Scanned with OKEN Scanner

Opusul numărului întreg a se notează prin $-a$. Observăm că numărul întreg $-a$ este negativ dacă a este pozitiv şi pozitiv dacă a este negativ.

Sîntem acum în măsură să arătăm că ecuaţia $x + a = b$, unde $a, b \in \mathbb{Z}$, are soluţie în $\mathbb{Z}$. Într-adevăr, $x = b + (-a)$ este unica soluţie a ecuaţei.

Numărul întreg $b + (-a)$ se notează prin $b - a$ şi se numeşte *diferenţa* dintre b şi a. Operaţia prin care oricărei perechi de numere întregi (b, a) i se asociază numărul întreg $b - a$ se numeşte *scădere*.

— *Înmulţirea numerelor întregi.* Se defineşte, acum, o altă operaţie pe $\mathbb{Z}$ numită *înmulţire* şi notată prin acelaşi simbol ca şi la numerele naturale.

Dacă $\overline{(m, n)}$ şi $\overline{(m', n')}$ sînt două numere întregi, se pune

$$\overline{(m, n)}, \overline{(m', n')} = \overline{(mm' + nn', mn' + m'n)}.$$

Numărul întreg $\overline{(mm' + nn', mn' + m'n)}$ se numeşte *produsul* numerelor întregi $\overline{(m, n)}$ şi $\overline{(m', n')}$, iar operaţia prin care celor două numere li se asociază produsul lor se numeşte *înmulţire*.

Operaţia de înmulţire este bine definită, adică, dacă $(m, n) \sim (m_1, n_1)$ şi $(m', n') \sim (m_1', n_1')$, atunci

$$\overline{(mm' + nn', mn' + m'n)} = \overline{(m_1m_1' + n_1n_1', m_1n' + m_1'n_1)}.$$

Într-adevăr, rezultă

$$m + n_1 = m_1 + n \text{ şi } m' + n_1' = m_1' + n'$$

Din prima relaţie se deduce

$$(m_1 + n_1)\, m_1' = (m_1 + n)\, m_1'$$

şi

$$(m_1 + n)\, n_1' = (m + n_1)\, n_1'.$$

Din relaţia $m' + n_1' = m_1' + n'$ se deduce

$$(m' + n_1')m = (m_1' + n')\, m \text{ şi } (m_1' + n')\, n = (m' + n_1')\, n.$$

Scanned with OKEN Scanner

Adunînd membru cu membru aceste relaţii, se obţine

$$(m + n_1)\, m_1' + (m_1 + n)n_1' + (m' + n_1')m + (m_1' + n')n =$$

$$= (m_1 + n)\, m_1' + (m + n_1)n_1' + (m_1' + n')\, m + (m' + n_1')n.$$

De aici

$$n_1 m' + m_1 n' + mm' + n'n =$$

$$= m_1 m_1' + n_1 n_1' + n'm + m'n$$

sau

$$(mm' + nn') + (m_1 n_1' + n_1 m_1') =$$

$$= (mn' + nm') + (m_1 m_1' + n_1 n_1'),$$

adică

$$(m'm + nn',\ mn' + m'n) \sim$$

$$\sim (m_1 m_1' + n_1 n_1',\ m_1 n_1' + m_1' n_1).$$

Fie reprezentanţi canonici ai numerelor întregi :
1° Produsul a două numere întregi pozitive :

$$\overline{(p, 0)}\ \ \overline{(p', 0)} = \overline{(pp', 0)},$$

ceea ce se scrie de asemenea

$$(+p)\,(+p') = +pp'.$$

2° Produsul a două numere întregi negative :

$$\overline{(0, q)}\ \ \overline{(0, q')} = \overline{(qq', 0)},$$

Scanned with OKEN Scanner

ceea ce se scrie, de asemenea

$$(-q)(-q') = +qq'.$$

3° Produsul a două numere întregi, unul pozitiv, altul negativ :

$$\overline{(p, 0)}\ \overline{(0, q)} = \overline{(0, pq)},$$

ceea ce se scrie de asemenea

$$(+p)(-q) = -pq.$$

Se obține, dealtfel, același rezultat permutînd factorii. Cînd un factor este nul, așa va fi și produsul.

Este clar, că produsul a două numere întregi nenule este nenul, adică dacă $a, b \in \mathbb{Z}$ și $a,\ b \neq 0$, atunci $ab \neq 0$.

Teorema 3.3. *Înmulțirea numerelor întregi are proprietățile :*

1) $aa' = a'a$, *oricare ar fi* $a,\ a' \in \mathbb{Z}$ *(comutativitatea)* ;

2) $a(a'a'') = (aa')a''$, *oricare ar fi* $a,\ a',\ a'' \in \mathbb{Z}$ *(asociativitatea)* ;

3) $a1 = 1a = a$, *oricare ar fi* $a \in \mathbb{Z}$ *(element neutru)* ;

4) $a(a' + a'') = aa' + aa''$, *oricare ar fi* $a,\ a',\ a'' \in \mathbb{Z}$ *(distributivitatea înmulțirii față de adunare)*.

Demonstrație. 1) și 2) rezultă imediat din cele de mai înainte.

3) Elementul neutru este $+1$ (notat încă 1), deoarece

$$(+1)(+p) = +p\ ,\ (+1)(-q) = -q.$$

4) Fie $a = \overline{(m,\ n)},\ a' = \overline{(m', n')},\ a'' = \overline{(m'', n'')}$; atunci

$$a(a'+a'') = \overline{(m,\ n)}\ \overline{(m'+m'',\ n'+n'')} =$$

$$= \overline{(mm'+mm''+nn'+nn'',\ mn'+mn''+nm'+nm'')}.$$

Fie

$$aa' = \overline{(m, n)}\,\overline{(m', n')} = \overline{(mm'+nn',\ mn'+nm')},$$

$$aa'' = \overline{(m, n)}\,\overline{(m'', n'')} = \overline{(mm''+nn'',\ mn''+nm'')},$$

de unde

$$aa'+aa'' =$$

$$= \overline{(nm'+nn'+mm''+nn'',\ mn'+nm'+mn''+nm'')}.$$

Cele două rezultate sînt egale, deci

$$a(a'+a'') = aa'+aa''.$$

— *Ordonarea numerelor întregi. Inegalități.*

Definiția 3.2. Fie a și b două numere întregi. Se spune că *a este mai mare decît b*, și se scrie $a > b$, dacă $a-b$ este pozitiv și nenul. Se spune că *a este mai mare sau egal cu b*, și se scrie $a \geqslant b$, dacă $a-b$ este pozitiv sau nul. Observăm că dacă $a = \overline{(m, n)}$ și $b = \overline{(p, q)}$, atunci $a \geqslant b$ dacă $m + q \geqslant n+p$.

1° Relația $>$ este tranzitivă.

2° Relația $\geqslant$ este reflexivă, antisimetrică și tranzitivă, adică este o relație de ordine.

Mai mult, două numere întregi a și b verifică una și numai una din relațiile

$$a > b,\ a = b \text{ sau } b > a,$$

adică mulțimea $\mathbb{Z}$ este *total ordonată*.

Dacă se consideră numerele întregi date prin reprezentanți canonici, rezultă

$$\overline{(p, 0)} > \overline{(p', 0)} \Leftrightarrow p > p',$$

Scanned with OKEN Scanner

$$\overline{(0, q)} > \overline{(0, q')} \Leftrightarrow q' > q.$$

Deci, orice număr pozitiv este mai mare decît zero, iar zero este mai mare decît orice număr negativ.

Din tranzitivitate rezultă că orice număr pozitiv este mai mare decît orice număr negativ, mai precis :

$$\overline{(p, 0)} > 0 > \overline{(0, q)} \text{ pentru } p, q \in \mathbb{N};\ p, q \neq 0.$$

Deci

$$\ldots < -n < \ldots < -2 < -1 < 0 < 1 < 2 < \ldots < n < \ldots$$

Se constată că aceste relaţii au proprietăţi analoage celor de la numere naturale. Iată, fără demonstraţie, cîteva proprietăţi ale lor :

1° Dacă $a, b, c \in \mathbb{Z}$ şi $a \geqslant b$, atunci $a + c \geqslant b + c$.

2° Dacă $a, b, c \in \mathbb{Z}$, $a \geqslant b$ şi $c \geqslant 0$, atunci $ac \geqslant bc$.

3° Dacă $a, b, c \in \mathbb{Z}$, $a \geqslant b$ şi $0 \geqslant c$, atunci $bc \geqslant ac$.

Să revenim la definiţia valorii absolute (sau a modulului) unui număr întreg. Avem :

$$|a| = \begin{cases} a, & \text{dacă } a > 0, \\ 0, & \text{dacă } a = 0, \\ -a, & \text{dacă } a < 0. \end{cases}$$

Propoziţia 3.4. *Dacă a şi b sînt numere întregi oarecare, atunci următoarele afirmaţii sînt adevărate :*

1) $|a| = 0 \Leftrightarrow a = 0$;

2) $|ab| = |a|\,|b|$;

3) $|a + b| \leqslant |a| + |b|$.

Scanned with OKEN Scanner

Demonstrație. 1) și 2) rezultă ușor. Să verificăm 3). Într-adevăr, dacă $a = 0$ sau $b = 0$, atunci evident

$$|a + b| = |a| + |b|.$$

Presupunem deci ambele numere întregi diferite de zero. Dacă $a > 0$ și $b > 0$, atunci $a + b > 0$, deci

$$|a + b| = |a| + |b|.$$

Dacă $a < 0$, $b < 0$, atunci $a + b < 0$, deci

$$|a + b| = -(a + b),\ |a| = -a,\ |b| = -b$$

și evident

$$|a + b| = |a| + |b|.$$

Fie $a > 0$, $b < 0$ și punînd $-b = b'$, avem

$$|a + b| = a - b'$$

și relația de verificat revine la următoarea:

$$|a - b'| < a + b'.$$

Dar $|a - b'|$ este egal cu $a - b'$ sau cu $-(a - b')$. Din $a < a + 2b'$ $(b' > 0)$ rezultă $a - b' < a + b'$, iar din $b' < b' + 2a$ $(a > 0)$, rezultă $-a + b' < a + b'$.

Așadar, în orice caz,

$$|a - b'| < a + b'.$$

Scanned with OKEN Scanner

Mulțimea $\mathbb{Z}$ a numerelor întregi are proprietăți aritmetice remarcabile. Ne vom opri în acest paragraf doar asupra cîtorva; altele se vor face în cap. IV.

Să dăm o teoremă analoagă teoremei împărțirii cu rest de la numerele naturale. Mai întîi să enunțăm lema lui Arhimede pentru numerele întregi.

Lema 3.5. *Dacă* $a, b \in \mathbb{Z}$, $a > 0$, *există* $n \in \mathbb{N}$ *astfel încît* $na > b$.

Demonstrație. Într-adevăr, dacă $b > 0$, această formulare este tocmai cea dată pentru numerele naturale, iar în cazul $b \leqslant 0$ este evidentă pentru orice $n \in \mathbb{N}$, deoarece $na > 0 \geqslant b$.

Teorema 3.6 *(teorema împărțirii cu rest). Dacă* a *și* b *sînt două numere întregi și* $b \neq 0$, *atunci există două numere întregi* q *și* r, *unic determinate, astfel încît*

$$a = bq + r, \quad 0 \leqslant r < |b|$$

(q *se numește cît, iar* r *rest).*

Demonstrație. Fie

$$M = \{t \geqslant 0 \mid \text{există } s \in \mathbb{Z},\ t = a - bs\}.$$

Avem că $M \neq \emptyset$. Într-adevăr, dacă se aplică lema lui Arhimede numerelor $|b| > 0$ și $-a$, se deduce că există un număr natural n, astfel încît $n|b| > -a$. Atunci numărul $t = n|b| + a > 0$ aparține lui M, unde se va lua, după caz, $s = n$ sau $s = -n$. Cum M este o mulțime nevidă de numere naturale, aceasta are un prim element $r \geqslant 0$. Dar $r < b$. În caz contrar, adică dacă $r \geqslant b$, se pot scrie relațiile

$$r = a - bq, \quad q \in \mathbb{Z},$$

$$0 \leqslant t = r - |b| = a - bs < r$$

cu $s = q + 1$ sau $s = q-1$, după caz. Astfel, ar exista un element $t \in M$, $t < r$, ceea ce este în contradicție cu faptul că r este primul element al mulțimii M. Există deci q și r, astfel încît

$$a = bq + r, \quad 0 \leqslant r < |b|.$$

Să demonstrăm unicitatea numerelor q și r. Într-adevăr, presupunem că q_1 și r_1 satisfac relațiile

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < |b|.$$

Atunci

$$0 = b\,(q-q_1) + (r-r_1),$$

de unde

$$|b|\,|q-q_1| = |r_1-r|.$$

Dacă $q-q_1 \neq 0$, atunci

$$|q-q_1| \geqslant 1, \quad |b| \cdot |q-q_1| \geqslant |b|,$$

de unde, de exemplu:

$$|b| > r_1 \geqslant r_1 - r = |r_1-r| \geqslant |b|,$$

adică se obține o contradicție. Deci

$$q = q_1 \text{ și } r = r_1.$$

Observații. 1. O variantă a teoremei 3.6. este următoarea: *Dacă $m, n \in \mathbb{Z}$, $n \neq 0$, atunci există $q, r \in \mathbb{Z}$, astfel încît*

$$m = nq + r \text{ și } |r| < |n|.$$

Pentru demonstrație, punem în teorema 3.6 $r = |r|$, r fiind $\geqslant 0$. Perechea de numere întregi din această variantă a teoremei nu este unică

pentru orice pereche de numere întregi m și n, $n \neq 0$. De exemplu : $-15 = (-4)\cdot 4 + 1$ și $|1| < |4|$ și $-15 = (-4)\cdot 3 + (-3)$ și $|-3| < |-4|$.

2. După cum se va vedea în cap. III, din teorema împărțirii cu rest rezultă proprietăți aritmetice remarcabile ale inelului $\mathbb{Z}$ al numerelor întregi.

§ 4. Construcția numerelor raționale

Fiind date două numere întregi a și b se pune problema dacă există un număr întreg c, astfel încît $a = bc$; cu alte cuvinte, dacă ecuația

$$a = bx$$

are soluție în mulțimea numerelor întregi. În general, această ecuație nu are întotdeauna soluție în $\mathbb{Z}$. Există două situații speciale :

1° $a \neq 0$, $b = 0$; în acest caz ecuația nu are nici o soluție, deoarece oricare ar fi $c \in \mathbb{Z}$, $bc = 0 \neq a$.

2° $a = b = 0$; caz de nedeterminare, deoarece oricare ar fi $c \in \mathbb{Z}$, $0c = 0$.

Așadar, vom presupune mereu că $b \neq 0$.

Ecuația $a = bx$ $(b \neq 0)$ are soluție în mulțimea $\mathbb{Z}$ a numerelor întregi dacă și numai dacă b este un divizor al lui a. În acest caz soluția este unică. Deci mulțimea $\mathbb{Z}$ nu are suficiente elemente încît orice ecuație de acest tip, pentru orice $a, b \in \mathbb{Z}$ $(b \neq 0)$, să aibă soluție în $\mathbb{Z}$. Se vor adăuga noi elemente la această mulțime, astfel încît noua mulțime obținută să satisfacă cerința impusă. Astfel, se va obține mulțimea $\mathbb{Q}$ a numerelor raționale. Pentru a obține această mulțime se procedează în felul următor.

Fie $\mathbb{Z}^*$ mulțimea numerelor întregi nenule și $\mathbb{Z} \times \mathbb{Z}^*$ mulțimea formată din toate perechile de numere întregi, a doua componentă a fiecărei perechi fiind nenulă, adică

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}.$$

Pe această mulțime se definește relația binară $\sim$ în modul următor :

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b.$$

Scanned with OKEN Scanner

Această relație este o relație de echivalență.

1° *Reflexivitatea*. Într-adevăr, $(a, b) \sim (a, b)$, deoarece $ab = ab$.

2°. *Simetria*. Dacă $(a, b) \sim (a', b')$, atunci $(a', b') \sim (a, b)$, deoarece din $ab' = a'b$ rezultă și $a'b = ab'$.

3° *Tranzitivitatea*. Dacă $(a, b) \sim (a', b')$ și $(a', b') \sim (a'', b'')$, atunci $(a, b) \sim (a'', b'')$. Într-adevăr, $ab' = a'b$ și $a'b'' = a''b'$. Înmulțind cu b'' ambii membri ai primei egalități și cu b pe ai celei de-a doua, se obțin $ab'b'' = a'bb''$ și $a'b''b = a''b'b$, de unde $ab'b'' \sim a''b'b$. Cum $b \neq 0$, rezultă $ab'' = a''b$, adică $(a, b) \sim (a'', b'')$.

Relația de echivalență împarte mulțimea $\mathbb{Z} \times \mathbb{Z}^*$ în clase de echivalență.

Definiția 4.1. Fiecare clasă de echivalență se numește *număr rațional*. Mulțimea numerelor raționale se notează cu $\mathbb{Q}$.

Toate perechile aparținînd aceleiași clase de echivalență sînt diverși reprezentanți ai acestei clase. Conform definiției adoptate, se spune că ele reprezintă același număr rațional.

Definiția 4.2. Cînd perechea (a, b), $b \neq 0$, de numere întregi are rolul de reprezentant al unui număr rațional, i se dă denumirea de *fracție*, primul său termen a se numește *numărător*, iar cel de-al doilea b se numește *numitor*.

O fracție se notează $\frac{a}{b}$ și se citește „a pe b“ sau „a supra b“. Relația $ab' = a'b$ exprimă faptul că perechile (a, b) și (a', b') aparțin aceleiași clase de echivalență, precum și faptul că fracțiile $\frac{a}{b}$ și $\frac{a'}{b'}$ reprezintă același număr rațional. Mulțimea de referință fiind mulțimea $\mathbb{Q}$ a numerelor raționale, iar fracțiile $\frac{a}{b}$ și $\frac{a'}{b'}$ reprezentînd același număr rațional, trebuie să le considerăm egale. În concluzie, pentru ca două fracții $\frac{a}{b}$ și $\frac{a'}{b'}$ să reprezinte

Scanned with OKEN Scanner

același număr rațional, altfel spus, pentru ca ele să fie egale, este necesar și suficient ca produsele ab' și $a'b$ să fie egale :

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b.$$
(în $\mathbb{Q}$) (în $\mathbb{Z}$)

Convenim, în continuare, să reprezentăm elementele lui $\mathbb{Q}$ prin fracții (prin fracțiile care le reprezintă).

Observație. Există o deosebire între numărul rațional $\frac{a}{b}$ și fracția $\frac{a}{b}$.

— *Valori absolute.* Fie $a, b, a', b' \in \mathbb{Z}$ $(b, b' \neq 0)$. Din egalitatea $ab' = a'b$ se deduce că :

1° Dacă a și b au același semn, atunci a' și b' au același semn. Altfel spus, dacă o fracție reprezentînd un anume număr rațional are ambii termeni de același semn, atunci orice altă fracție ce reprezintă același număr rațional are cei doi termeni ai săi de același semn. Se spune atunci că numărul rațional este pozitiv.

2° Dacă a și b sînt de semne contrare, atunci a' și b' sînt de semne contrare. Se spune în acest caz că numărul rațional este negativ.

Din $ab' = a'b$ rezultă $|a|\,|b'| = |a'|\,|b|$ și de aici

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow \frac{|a|}{|b|} = \frac{|a'|}{|b'|}.$$

Așadar, dacă fracțiile $\frac{a}{b}$ și $\frac{a'}{b'}$ reprezintă același număr rațional și fracțiile $\frac{|a|}{|b|}$ și $\frac{|a'|}{|b'|}$ reprezintă același număr rațional. Acest ultim număr rațional va fi numit *valoare absolută* a lui $\frac{a}{b}$ și va fi notat cu $\left|\frac{a}{b}\right|$.

Scanned with OKEN Scanner

Examinăm succesiv cazul cînd numărul raţional $\frac{a}{b}$ este pozitiv şi cazul cînd $\frac{a}{b}$ este negativ.

1° Un *număr raţional pozitiv* este de forma $\frac{|a|}{|b|}$ sau $\frac{-|a|}{-|b|}$. Cînd $\frac{a}{b}$ este pozitiv, convenim să punem

$$\frac{a}{b} = +\left|\frac{a}{b}\right|, \text{ unde } \left|\frac{a}{b}\right| = \frac{|a|}{|b|}.$$

Dealtfel, în general, semnul + se omite.

2° Un *număr raţional negativ* este de forma $\frac{+|a|}{-|b|} = \frac{-|a|}{+|b|}$.

Cînd numărul raţional este negativ, convenim să punem

$$\frac{a}{b} = -\left|\frac{a}{b}\right|, \text{ unde } \left|\frac{a}{b}\right| = \frac{|a|}{|b|}.$$

3° *Numărul nul.* Cînd $a = 0$, atunci $ab' = 0$ şi din $a'b = 0$ $(b \neq 0)$ rezultă $a' = 0$. Deci, dacă o fracţie are numărătorul nul, atunci orice fracţie egală cu aceasta are de asemenea numărătorul nul. Se spune că acest număr raţional este nul, se notează cu 0 iar valoarea sa absolută este 0. I se poate atribui semnul + sau —, la alegere, dar acesta în general se omite.

— *Amplificări. Simplificări. Fracţii ireductibile.*

Definiţia 4.3. *A amplifica* o fracţie $\frac{a}{b}$ înseamnă a înmulţi ambii termeni ai săi a şi b cu acelaşi număr întreg nenul.

Scanned with OKEN Scanner

A simplifica o fracție $\frac{a}{b}$ înseamnă a împărți ambii termeni ai săi a și b printr-un număr care este un divizor comun al lor.

Dacă $t \in \mathbb{Z}$ $(t \neq 0)$, atunci după definiție rezultă

$$\frac{a}{b} = \frac{at}{bt}$$

Deci, prin amplificări sau simplificări o fracție nu se schimbă. Cînd $t = -1$, putem scrie

$$\frac{a}{b} = \frac{(-1) \times a}{(-1) \times b}.$$

Unul dintre b sau $-b$ este pozitiv și deci un număr rațional poate fi reprezentat printr-o fracție cu numitor pozitiv. Astfel, m și n fiind numere întregi pozitive, avem

$$\frac{-m}{n} = -\frac{m}{n}, \qquad \frac{+m}{n} = +\frac{m}{n}.$$

În concluzie, un număr rațional pozitiv se reprezintă ca $+\frac{m}{n}$, iar unul negativ ca $-\frac{m}{n}$, valoarea sa absolută $\frac{m}{n}$ exprimîndu-se printr-o fracție ai cărei termeni sînt numere întregi pozitive (adică numere naturale). Deoarece simplificarea privește numai valorile absolute, toate fracțiile care vor interveni în legătură cu aceasta au termeni pozitivi.

Fie $\frac{m}{n}$ o fracție și $d = (m, n)$ c.m.m.d.c. al lui m și n. Atunci $m = dp$ și $n = dq$, unde p și q sînt prime între ele. Deci

$$\frac{m}{n} = \frac{dp}{dq} = \frac{p}{q}, \qquad (p, q) = 1.$$

Scanned with OKEN Scanner

Fracția $\frac{p}{q}$ cu $(p, q) = 1$ se numește *ireductibilă*. Așadar, orice fracție este egală cu o fracție ireductibilă.

Fie $\frac{p}{q}$ o fracție ireductibilă. Ne propunem să descriem toate fracțiile $\frac{x}{y}$ egale cu $\frac{p}{q}$.

Teorema 4.1. *Pentru ca o fracție* $\frac{x}{y}$ *să fie egală cu o fracție* $\frac{p}{q}$ *ireductibilă, este necesar și suficient ca* $\frac{x}{y}$ *să se obțină prin amplificare din* $\frac{p}{q}$.

Demonstrație. Fie $\frac{x}{y} = \frac{p}{q}$; atunci $xq = yp$. De aici se obține $q \mid yp$ și cum $(q, p) = 1$, rezultă $q \mid y$. Există deci $k \in \mathbb{N}$, $k \neq 0$, astfel încît $y = qk$ care, înlocuit în egalitatea $xq = yp$, ne dă $xq = qkp$. Dar $q \neq 0$, de unde $x = kp$. Așadar, $\frac{x}{y}$ se obține din $\frac{p}{q}$ prin amplificare cu k. Dacă considerăm o fracție de forma $\frac{pk}{qk}$, aceasta este, evident, egală cu $\frac{p}{q}$.

Fie o fracție $\frac{a}{b}$ cu $a, b \in \mathbb{Z}$. O astfel de fracție este ireductibilă dacă fracția $\frac{|a|}{|b|}$ este ireductibilă.

Numărul rațional pozitiv $+\frac{m}{n}$ are două expresii ireductibile: $\frac{p}{q}$ și $\frac{-p}{-q}$. Numărul rațional negativ

$-\frac{m}{n}$ are două expresii ireductibile : $\frac{-p}{q}$ și $\frac{p}{-q}$. Totodată, printre fracțiile ireductibile ce dau același număr rațional, există una al cărei numitor să fie pozitiv, fie aceasta $\frac{p}{q}$ sau $\frac{-p}{q}$. Atunci dacă $\frac{m}{n}$ este un număr rațional pozitiv, există $k \in \mathbb{Z}$ încît $\frac{m}{n} = \frac{kp}{kq}$, iar dacă $-\frac{m}{n}$ este negativ, există $r \in \mathbb{Z}$ încît $-\frac{m}{n} = \frac{-rp}{rq}$.

Observație. Convenim să identificăm numărul rațional $\frac{q}{1}$ reprezentat de fracția ireductibilă $\frac{q}{1}$ (și deci de toate fracțiile $\frac{nq}{n}$, $n \in \mathbb{Z}$ $n \neq 0$) cu numărul întreg q. Această convenție se justifică în continuare.

Vom da acum o reprezentare grafică a mulțimii numerelor raționale, în care să punem în evidență fracțiile ce definesc același număr rațional. Considerăm două axe de coordonate, perpendiculare (vezi fig. 2). Fiecare fracție $\frac{a}{b}$ are ca imagine un punct de abscisă b (numitorul) și ordonată a (numărătorul). Presupunem $b > 0$, a fiind pozitiv, negativ sau nul. Toate fracțiile care reprezintă același număr rațional au imaginile situate pe aceeași dreaptă. Fiecare număr rațional apare scris la baza unei astfel de direcții.

— *Aducerea fracțiilor la același numitor.* Fie $\frac{a}{b}$ și $\frac{c}{d}$ două fracții. Putem presupune $b, d > 0$, numărătorii a și c pot fi pozitivi, negativi sau nuli. Fie m un multiplu comun al numitorilor (se poate lua, în particular, c.m.m.m.c.). Atunci $m = bb'$ și $m = dd'$, cu $b, d \in \mathbb{Z}$ iar fracțiile date se pot scrie

$$\frac{a}{b} = \frac{ab'}{bb'} \text{ și } \frac{c}{d} = \frac{cd'}{dd'},$$

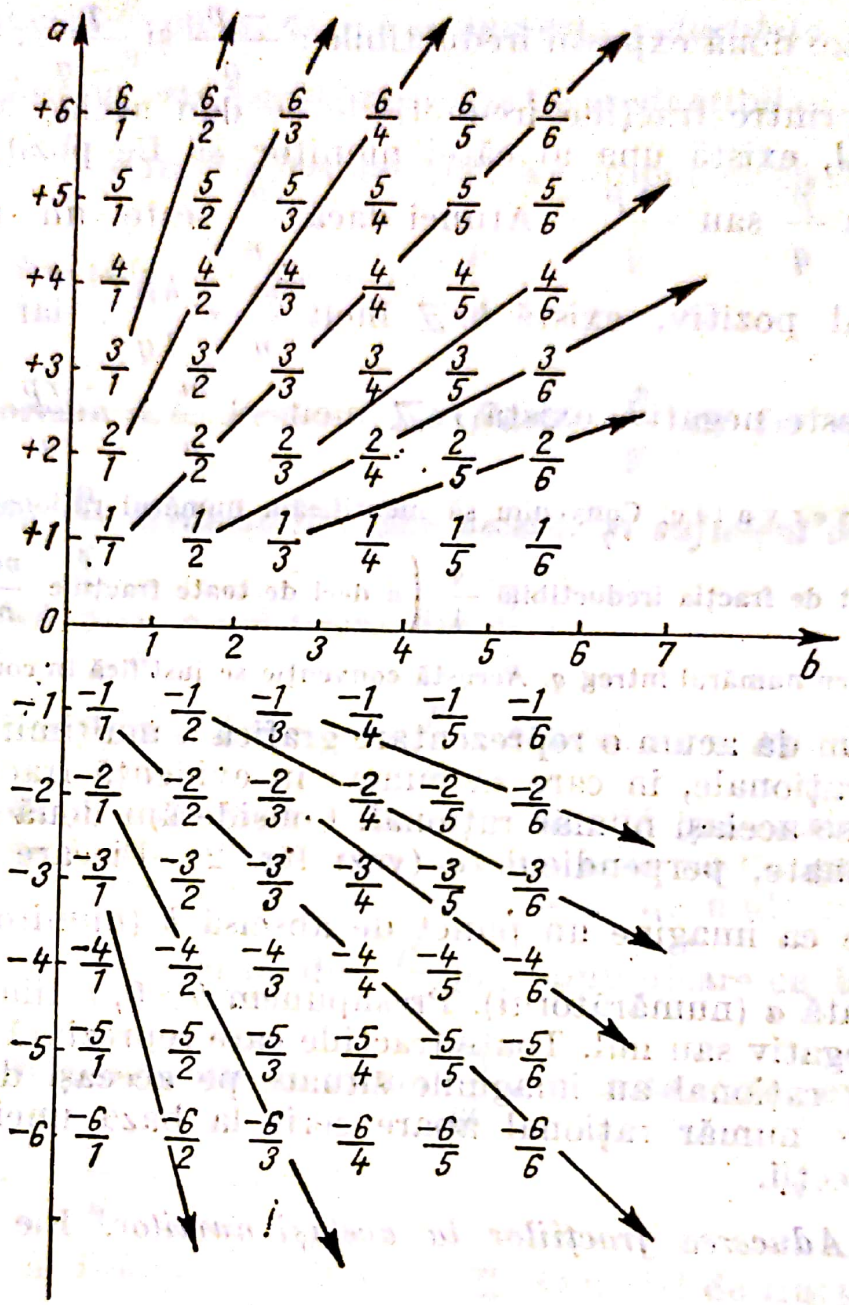


Fig. 2

apoi, punînd $x = ab$ şi $y = cd$, se obţin

$$\frac{a}{b} = \frac{x}{m} \text{ şi } \frac{c}{d} = \frac{y}{m}.$$

A înlocui $\frac{a}{b}$ și $\frac{c}{d}$ prin $\frac{x}{m}$ și $\frac{y}{m}$ înseamnă, prin definiție, *a aduce fracțiile la același numitor*.

Prin același procedeu, se pot considera și mai multe fracții (trei, patru etc.).

— *Adunarea numerelor raționale.* Pe mulțimea $\mathbb{Q}$ a numerelor raționale vom defini o operație pe care o numim adunare și pe care o notăm, de asemenea, cu $+$.

Definiția 4.4. Dacă $\frac{a}{b}$ și $\frac{a'}{b'}$ sînt două numere raționale, punem

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}.$$

Numărul rațional $\frac{ab' + a'b}{bb'}$ se numește *suma* numerelor raționale $\frac{a}{b}$ și $\frac{a'}{b'}$, iar operația prin care celor două numere $\frac{a}{b}$ și $\frac{a'}{b'}$ li se asociază suma lor se numește *adunare*. Această operație se numește de obicei *adunarea fracțiilor*.

Se pune problema dacă adunarea este bine definită, adică dacă

$$(a, b) \sim (a_1, b_1) \text{ și } (a', b') \sim (a'_1, b'_1),$$

atunci

$$\frac{ab' + a'b}{bb'} = \frac{a_1b'_1 + a'_1b_1}{b_1b'_1}.$$

Într-adevăr, avem $ab_1 = a_1b$ și $a'b'_1 = a'_1b'$. Înmulțind ambii membri ai primei egalități cu $b'b'_1$ și pe ai celei de-a doua cu bb_1, se obțin relațiile

$$ab_1b'b'_1 = a_1bb'b'_1 \text{ și } a'b'_1bb_1 = a'_1b'bb_1.$$

Adunînd membru cu membru aceste două egalităţi şi scoţînd factor comun, rezultă

$$(ab' + a'b)b_1b_1' = (a_1b_1' + a_1'b_1)bb',$$

adică

$$(ab' + a'b, bb') = (a_1b_1' + a_1'b_1, b_1b_1').$$

Cînd fracţiile care se adună au acelaşi numitor, să zicem $m \neq 0$, formula de adunare a fracţiilor se scrie

$$\frac{a}{m} = \frac{a'}{m} = \frac{am' + a'm}{mm} = \frac{(a + a')m}{mm} = \frac{a + a'}{m}.$$

Teorema 4.2. *Adunarea numerelor raţionale are proprietăţile :*

1) $\frac{a}{b} + \frac{a'}{b'} = \frac{a'}{b'} + \frac{a}{b}$, *oricare ar fi* $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Q}$;

2) $\frac{a}{b} + \left(\frac{a'}{b'} + \frac{a''}{b''}\right) = \left(\frac{a}{b} + \frac{a'}{b'}\right) + \frac{a''}{b''}$, *oricare ar fi* $\frac{a}{b}, \frac{a'}{b'}, \frac{a''}{b''} \in \mathbb{Q}$;

3) $\frac{a}{b} + 0 = 0 + \frac{a}{b} = \frac{a}{b}$, *oricare ar fi* $\frac{a}{b} \in \mathbb{Q}$;

4) *pentru orice* $\frac{a}{b} \in \mathbb{Q}$, avem $\frac{a}{b} + \frac{-a}{b} = \frac{-a}{b} + \frac{a}{b} = 0$.

Demonstraţie. În demonstraţia acestor proprietăţi numerele raţionale vor fi reprezentate prin fracţii cu acelaşi numitor şi atunci acestea se deduc din proprietăţile analoage de la numerele întregi.

1) Dacă $\frac{a}{b} = \frac{c}{m}$ și $\frac{a'}{b'} = \frac{c'}{m}$, atunci

$$\frac{a}{b} + \frac{a'}{b'} = \frac{c}{m} + \frac{c'}{m} = \frac{c + c'}{m}$$

și

$$\frac{a'}{b'} + \frac{a}{b} = \frac{c'}{m} + \frac{c}{m} = \frac{c' + c}{m}$$

sînt egale, deoarece $c + c' = c' + c$ (în $\mathbb{Z}$).

2) Dacă $\frac{a}{b} = \frac{c}{m}$, $\frac{a'}{b'} = \frac{c'}{m}$, $\frac{a''}{b''} = \frac{c''}{m}$, atunci

$$\frac{a}{b} + \left(\frac{a'}{b'} + \frac{a''}{b''}\right) = \frac{c + (c' + c'')}{m}$$

și

$$\left(\frac{a}{b} + \frac{a'}{b'}\right) + \frac{a''}{b''} = \frac{(c + c') + c''}{m}$$

sînt egale, deoarece $c + (c' + c'') = (c + c') + c''$.

3) Toate fracțiile cu numărătorul nul sînt egale între ele și dau numărul 0.

Avem $\frac{a}{b} + 0 = \frac{a}{b} + \frac{0}{b} = \frac{a + 0}{b} = \frac{a}{b}$.

4) Fie $\frac{a}{b} \in \mathbb{Q}$, atunci $\frac{-a}{b} \in \mathbb{Q}$ și

$$\frac{a}{b} + \frac{-a}{b} = \frac{a + (-a)}{b} = \frac{0}{b} = 0.$$

Numărul $\frac{-a}{b}$ este opusul numărului $\frac{a}{b}$ și-l notăm $-\frac{a}{b}$.

Scanned with OKEN Scanner

Fie ecuația

$$x + \frac{a}{b} = \frac{a'}{b'}\ ;\ \frac{a}{b}\ ,\ \frac{a'}{b'} \in \mathbb{Q}.$$

Această ecuație are o soluție unică în $\mathbb{Q}$, care este

$$x = \frac{a'}{b'} + \left(-\frac{a}{b}\right), \text{ unde } -\frac{a}{b} = \frac{-a}{b}\ .$$

x se numește *diferența* dintre $\frac{a'}{b'}$ și $\frac{a}{b}$ și se notează

$$\frac{a'}{b'} - \frac{a}{b}\ .$$

Operația prin care la două numere raționale se asociază diferența lor se numește *scădere*.

— *Înmulțirea numerelor raționale.* Vom defini o altă operație pe $\mathbb{Q}$ pe care o numim *înmulțire* și pe care o notăm prin același semn ca și la numerele întregi și naturale.

Definiția 4.5. Dacă $\frac{a}{b}$ și $\frac{a'}{b'}$ sînt două numere raționale, se va pune

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}\ .$$

Numărul rațional $\frac{aa'}{bb'}$ se numește *produsul* numerelor raționale $\frac{a}{b}$ și $\frac{a'}{b'}$, iar operația prin care celor două numere $\frac{a}{b}$ și $\frac{a'}{b'}$ li se asociază produsul lor se numește

înmulțire. Această operație se numește de obicei *înmulțirea fracțiilor*.

Să verificăm că operația de înmulțire este bine definită, adică dacă $(a, b)\sim(a_1, b_1)$ și $(a', b')\sim(a'_1, b'_1)$, atunci

$$\frac{aa'}{bb'} = \frac{a_1a'_1}{b_1b'_1}.$$

Într-adevăr, avem $ab_1 = a_1b$ și $a'b'_1 = a'_1b'$. Înmulțind membru cu membru aceste două egalități, se obține $ab_1a'b'_1 = a_1ba'_1b'$ sau $(aa')(b_1b'_1) = (a_1a'_1)(bb')$, de unde

$$(aa', bb')\sim(a_1a'_1, b_1b'_1).$$

Fie acum $m \neq 0$; atunci $\frac{m}{m} = \frac{1}{1}$ și după convenția făcută $\frac{1}{1} = 1$. Acest număr rațional îl vom numi *numărul rațional unitate*, sau *unu*, ca și la numerele întregi.

Teorema 4.3. *Înmulțirea numerelor raționale are proprietățile*:

1) $\frac{a}{b}\,\frac{a'}{b'} = \frac{a'}{b'}\,\frac{a}{b}$, *oricare ar fi* $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Q}$;

2) $\frac{a}{b}\left(\frac{a'}{b'}\,\frac{a''}{b''}\right) = \left(\frac{a}{b}\,\frac{a'}{b'}\right)\frac{a''}{b''}$, *oricare ar fi*

$$\frac{a}{b}, \frac{a'}{b'}, \frac{a''}{b''} \in \mathbb{Q};$$

3) $\frac{a}{b} \cdot 1 = 1 \cdot \frac{a}{b} = \frac{a}{b}$, *oricare ar fi* $\frac{a}{b} \in \mathbb{Q}$;

4) *dacă* $\frac{a}{b} \neq 0$, *atunci* $\frac{b}{a} \in \mathbb{Q}$ *și*

Scanned with OKEN Scanner

$$\frac{a}{b}\,\frac{b}{a} = \frac{b}{a}\,\frac{a}{b} = 1.$$

5) $\dfrac{a}{b}\left(\dfrac{a'}{b'} + \dfrac{a''}{b''}\right) = \dfrac{a}{b}\,\dfrac{a'}{b'} + \dfrac{a}{b}\,\dfrac{a''}{b''}$, *oricare ar fi*

$$\frac{a}{b},\ \frac{a'}{b'},\ \frac{a''}{b''} \in \mathbb{Q}.$$

Demonstrație. 1) Produsele $\dfrac{a}{b}\,\dfrac{a'}{b'} = \dfrac{aa'}{bb'}$ și $\dfrac{a'}{b'}\,\dfrac{a}{b} = \dfrac{a'a}{b'b}$ sînt egale, deoarece $aa' = a'a$ și $bb' = b'b$ (după comutativitatea din $\mathbb{Z}$).

2) Produsele $\dfrac{a}{b}\left(\dfrac{a'}{b'}\,\dfrac{a''}{b''}\right) = \dfrac{a(a'a'')}{b(b'b'')}$ și $\left(\dfrac{a}{b}\,\dfrac{a'}{b'}\right)\dfrac{a''}{b''} = \dfrac{(aa')a''}{(bb')b''}$ sînt egale deoarece $a(a'a'') = (aa')a''$ și $b(b'b'') = (bb')b''$ sînt egale (asociativitatea din $\mathbb{Z}$).

3) $\dfrac{a}{b}\cdot 1 = \dfrac{a}{b}\cdot\dfrac{1}{1} = \dfrac{a\cdot 1}{b\cdot 1} = \dfrac{a}{b}$.

4) Dacă $\dfrac{a}{b} \neq 0$, atunci $a \neq 0$ și deci $\dfrac{b}{a} \in \mathbb{Q}$. Mai mult,

$$\frac{a}{b}\cdot\frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1.$$

5) Fie $\dfrac{a'}{b'} = \dfrac{c'}{m}$ și $\dfrac{a''}{b''} = \dfrac{c''}{m}$. Atunci

$$\frac{a}{b}\left(\frac{a'}{b'} + \frac{a''}{b''}\right) = \frac{a}{b}\left(\frac{c'}{m} + \frac{c''}{m}\right) = \frac{a}{b}\cdot\frac{c' + c''}{m} = \frac{a(c' + c'')}{bm}$$

iar

$$\frac{a}{b}\frac{a'}{b'}+\frac{a}{b}\frac{a''}{b''}=\frac{a}{b}\cdot\frac{c'}{m}+\frac{a}{b}\frac{c''}{m}=$$

$$=\frac{ac'}{bm}+\frac{ac''}{bm}=\frac{ac'+ac''}{bm}\cdot$$

Cele două expresii sînt egale, deoarece în $\mathbb{Z}$ are loc

$$a(c'+c'')=ac'+ac''.$$

Definiția 4.6. Dacă $\frac{a}{b}\neq 0$, atunci numărul $\frac{b}{a}\neq 0$ are proprietatea

$$\frac{a}{b}\frac{b}{a}=\frac{b}{a}\frac{a}{b}=1.$$

Acesta este *inversul* lui $\frac{a}{b}$ și se notează prin $\left(\frac{a}{b}\right)^{-1}$.

Sîntem acum în măsură să demonstrăm că o ecuație de forma

$$x\cdot\frac{a}{b}=\frac{c}{d},\ \text{unde}\ \frac{a}{b},\ \frac{c}{d}\in\mathbb{Q}\ \text{iar}\ \frac{a}{b}\neq 0$$

are soluție în $\mathbb{Q}$.

Într-adevăr, $x=\frac{c}{d}\left(\frac{a}{b}\right)^{-1}=\frac{c}{d}\cdot\frac{b}{a}=\frac{cb}{da}$ este unica soluție a ecuației.

Numărul rațional $\frac{c}{d}\cdot\left(\frac{a}{b}\right)^{-1}$ se numește *cîtul* lui $\frac{c}{d}$ prin $\frac{a}{b}$, iar operația prin care la cele două numere raționale se asociază cîtul lor se numește *împărțire*.

Definiția 4.7. Fie $\frac{a}{b}$ și $\frac{c}{d} \in \mathbb{Q}$. Spunem că $\frac{a}{b}$ *este mai mare ca* $\frac{c}{d}$ și scriem $\frac{a}{b} > \frac{c}{d}$, dacă $\frac{a}{b} - \frac{c}{d}$ este pozitiv și nenul. Spunem că $\frac{a}{b}$ *este mai mare sau egal cu* $\frac{c}{d}$ și scriem $\frac{a}{b} \geqslant \frac{c}{d}$, dacă $\frac{a}{b} - \frac{c}{d}$ este pozitiv sau nul.

Reprezentăm $\frac{a}{b}$ și $\frac{c}{d}$ ca fracții de același numitor pozitiv:

$$\frac{a}{b} = \frac{a'}{m}, \quad \frac{c}{d} = \frac{c'}{m}, \quad m > 0.$$

Fie diferența $\frac{a}{b} - \frac{c}{d} = \frac{a' - c'}{m}$; m fiind pozitiv, această diferență are semnul numărătorului $a' - c'$. Se deduce atunci

$$\frac{a}{m} > \frac{c'}{m} \Leftrightarrow a' > c',$$

$$\frac{a'}{m} \geqslant \frac{c'}{m} \Leftrightarrow a' \geqslant c'.$$

Toate proprietățile demonstrate pentru $\mathbb{Z}$, referitor la relațiile $>$ și $\geqslant$, sînt adevărate și pentru $\mathbb{Q}$, acestea extinzîndu-se fără dificultate. Lăsăm, ca exercițiu, reformularea și demonstrarea lor pentru numerele raționale.

Convenția pe care am făcut-o și anume $\frac{q}{1} = q$ permite să efectuăm calcule cu numere raționale chiar și

atunci cînd acestea sînt numere întregi (acestea fiind luate ca fracţii de numitor 1).

Să considerăm ecuaţia $xb = a$, $a, b \in \mathbb{Z}$, $b \neq 0$. Această ecuaţie are o unică soluţie în $\mathbb{Q}$ şi anume $\frac{a}{1}\left(\frac{b}{1}\right)^{-1} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{b}$. Prin urmare, conform definiţiei împărţirii numerelor raţionale putem concepe fracţia $\frac{a}{b}$ drept cîtul lui a prin b.

Observaţii. 1. Cu toată lărgirea repetată a noţiunii de număr de la numărul natural pînă la numărul raţional, există operaţii simple derivate din operaţiile fundamentale, care nu sînt posibile în mulţimea numerelor raţionale. Vom arăta de exemplu, că nu există nici un număr raţional a al cărui pătrat să fie egal cu 2.

Într-adevăr, să presupunem, prin absurd, că $a = \frac{p}{q}$ are proprietatea că

$$\frac{p^2}{q^2} = 2.$$

Putem presupune că numerele p şi q sînt naturale, deoarece nu intră în egalitatea precedentă decît prin pătratul lor. Mai mult încă, putem presupune că fracţia $\frac{p}{q}$ este ireductibilă, adică numerele p şi q nu au divizori comuni afară de 1. Avem

$$p^2 = 2q^2.$$

De aici $2 \mid p^2$, deci $2 \mid p$ sau $p = 2r$. Dar din $p^2 = 2q^2$ rezultă $4r^2 = 2q^2$ sau $2r^2 = q^2$, deci $2 \mid q^2$, adică $2 \mid q$. Aşadar, $2 \mid p$ şi $2 \mid q$, ceea ce contrazice alegerea lui p şi q. În concluzie, nu există nici un număr raţional al cărui pătrat să fie egal cu 2.

Aşadar, se impune ca mulţimea $\mathbb{Q}$ a numerelor raţionale să fie lărgită. Aceasta se completează cu numere iraţionale, obţinîndu-se astfel mulţimea $\mathbb{R}$ a numerelor reale. Fundamentarea matematică riguroasă a teoriei numerelor reale nu constituie obiectul acestei cărţi.

2. Să considerăm, acum, problema rezolvării unei ecuaţii de gradul al doilea cu coeficienţi reali. Mulţimea numerelor reale nu se dovedeşte suficientă pentru a putea găsi rădăcini ale oricărei ecuaţii de acest tip. Cea mai simplă ecuaţie de gradul al doilea care nu are rădăcini reale este

$$x^2 + 1 = 0.$$

Se pune problema lărgirii conceptului de număr real, introducînd o mulțime de numere mai bogată, în așa fel ca ecuația de mai sus să aibă soluție. În această nouă mulțime ridicarea la o putere oarecare va avea întotdeauna sens. Noua mulțime care se obține va fi mulțimea $\mathbb{C}$ a numerelor complexe. Studiul acestei mulțimi nu constituie obiectul cărții de față.

Problematica pe care o ridică această carte nu necesită cititorului alte cunoștințe referitoare la numerele reale și complexe, în afara celor obținute în școală.

§ 5. Structuri algebrice

— *Noțiunea de grup*

Definiția 5.1. Se numește *grup* o mulțime nevidă G înzestrată cu o operație algebrică

$$* : G \times G \to G$$

asociativă, cu element neutru și astfel încît orice element din G este simetrizabil. Se mai spune că în acest caz s-a dat o *structură de grup*. Dacă, în plus, operația este comutativă, se spune că grupul G este *comutativ*.

În general, într-un grup oarecare G, elementul $x * y$ se notează, de obicei, cu xy și se numește *produsul* lui x cu y, sau cu $x + y$ și se numește *suma* lui x cu y. După caz, se spune că grupul G este *multiplicativ*, respectiv *aditiv*. Se rezervă, în general, notația aditivă pentru grupurile comutative. Mulțimea G va desemna, în același timp, mulțimea elementelor grupului și grupul însuși, adică mulțimea înzestrată cu operația algebrică.

Dacă G și G' sînt grupuri, de exemplu, multiplicative, o aplicație $\varphi : G \to G'$ se numește *omomorfism* de grupuri dacă

$$\varphi(xy) = \varphi(x)\varphi(y), \text{ oricare ar fi } x, y \in G.$$

Dacă aplicația φ este injectivă, surjectivă, bijectivă (inversabilă), atunci omomorfismul φ se numește *monomorfism*, *epimorfism*, *respectiv izomorfism*.

Scanned with OKEN Scanner

Exemple de grupuri

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$ sînt grupuri comutative în raport cu operaţia de adunare din $\mathbb{Z}$ $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$ respectiv.

2. $\mathbb{Q}^* = \{x \in \mathbb{Q} \mid x \neq 0\}$, adică mulţimea numerelor raţionale nenule, înzestrată cu operaţia de înmulţire este grup comutativ.

3. $\mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\}$, adică mulţimea numerelor reale pozitive înzestrată cu operaţia de înmulţire este grup comutativ.

4. Mulţimea $S(M) = \{f \mid f : M \to M$, bijectivă$\}$ este grup în raport cu operaţia de compunere a funcţiilor. Acest grup se numeşte *grupul permutărilor* mulţimii M. În general, acesta este un grup necomutativ. El este comutativ dacă şi numai dacă M are cel mult două elemente. Lăsăm ca exerciţiu verificarea acestui fapt.

5. Mulţimea $M = \{-1, 1\} \subset \mathbb{Z}$ pe care este definită operaţia de înmulţire a numerelor întregi este un grup comutativ. Acesta este definit prin următorul tabel:

$\cdot$	-1	1
-1	1	-1
1	-1	1

Observaţie. Se poate defini orice grup finit G cu ajutorul unui tabel de acest tip. Dacă G este un grup multiplicativ cu n elemente, tabla sa de înmulţire este un tabel pătrat de tip $n \times n$ în care se înscriu mai întîi la capătul liniilor şi coloanelor o listă cu cele n elemente ale lui G. În acest tabel termenul care se găseşte la intersecţia liniei x şi a coloanei y este produsul xy în G.

Exemple de omomorfisme

Funcţia $\ln : \mathbb{R}_+^* \to \mathbb{R}$ este un omomorfism de grupuri, pentru că

$$\ln(xy) = \ln x + \ln y.$$

Această funcţie este chiar un izomorfism, inversa sa fiind funcţia $x \to e^x$ care este de asemenea un omomorfism de grupuri (deoarece $e^{x+y} = e^x e^y$).

Funcţia $\varphi : \mathbb{Z} \to \{-1, 1\}$, definită prin

$$\varphi(x) = \begin{cases} 1, \text{ dacă } x \text{ este par,} \\ -1, \text{ dacă } x \text{ este impar,} \end{cases}$$

este un omomorfism surjectiv de grupuri de la grupul aditiv al numerelor întregi la grupul multiplicativ $\{-1, 1\}$, după cum se poate verifica cu uşurinţă. De asemenea, funcţia $\psi : \mathbb{Z} \to \mathbb{Z}$, definită prin $\psi(x) = 2x$ este un omomorfism injectiv de grupuri de la grupul aditiv al numerelor întregi în el însuşi.

Scanned with OKEN Scanner

Propoziția 5.1. *Dacă G și G' sînt două grupuri, e și e' elementele neutre ale lui G, respectiv G' și $\varphi : G \to G'$ un omomorfism, atunci :*

1) $\varphi(e) = e'$;

2) *oricare* $x \in G \Rightarrow \varphi(x^{-1}) = (\varphi(x))^{-1}$.

Demonstrație. 1) Avem

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e).$$

Înmulțind la stînga cu $(\varphi(e))^{-1}$, rezultă

$$e' = \varphi(e).$$

2) Avem

$$e' = \varphi(e) = \varphi(xx^{-1}) = \varphi(x)\ \varphi(x^{-1}).$$

De asemenea $e' = \varphi(x^{-1})\varphi(x)$. Aceste două relații dau că $\varphi(x^{-1})$ este inversul lui $\varphi(x)$.

Definiția 5.2. Fie G un grup. O submulțime nevidă H a lui G se spune că formează un *subgrup* al lui G dacă operația algebrică de pe G induce o operație algebrică pe H împreună cu care H este grup.

Propoziția 5.2. *Fie G un grup și H o parte nevidă a lui G. Atunci următoarele afirmații sînt echivalente :*

1) *H este subgrup al lui G.*

2) *Sînt satisfăcute următoarele condiții :*

   1° *pentru orice $x, y \in H$ rezultă $xy \in H$;*

   2° *$e \in H$ (e fiind elementul neutru al lui G) ;*

   3° *pentru orice $x \in H$ rezultă $x^{-1} \in H$.*

3) *Pentru orice $x, y \in H$ rezultă $xy^{-1} \in H$.*

Demonstrație. 1) $\Rightarrow$ 2). Faptul că operația de pe G induce o operație pe H, înseamnă că pentru orice $x, y \in H$ rezultă $xy \in H$, adică condiția 1°. Fie acum e' elementul neutru al lui H ; atunci $e'e' = e'$. Dacă $(e')^{-1}$ este inversul lui e' în G, atunci $e' = e'(e')^{-1} = e$ și deci $e \in H$, adică condiția 2°. Fie $x \in H$ și x' inversul lui x în H. Atunci $xx' = x'x = e$ și deci x' este inversul lui x în G. Așadar, $x^{-1} \in H$ și

Scanned with OKEN Scanner

deci 3°. 2) $\Rightarrow$ 3). Dacă $x, y \in H$, conform cu 3°, rezultă $y^{-1} \in H$, şi, conform cu 1°, $xy^{-1} \in H$.

3) $\Rightarrow$ 1) Dacă $x \in H$, atunci $xx^{-1} = e \in H$ şi $x^{-1} = ex^{-1} \in H$. De asemenea, dacă $y \in H$ şi cum $y^{-1} \in H$, se obţine

$$xy = x(y^{-1})^{-1} \in H.$$

De exemplu, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sînt subgrupuri unul în altul faţă de operaţia de adunare. De asemenea $\{-1, 1\}$ cu operaţia de înmulţire este subgrup al grupului multiplicativ $\mathbb{Q}^*$, care la rîndul său este subgrup al grupului multiplicativ $\mathbb{R}^*$.

Vom caracteriza subgrupurile grupului aditiv al numerelor întregi.

Propoziţia 5.3. *Fie n un număr întreg şi pozitiv şi $n\mathbb{Z}$ mulţimea formată din multiplii întregi ai lui n:*

$$\ldots, -2n, -n, 0, n, 2n, \ldots$$

Atunci:

1) *$n\mathbb{Z}$ este un subgrup al grupului aditiv $\mathbb{Z}$;*

2) *orice subgrup al grupului aditiv $\mathbb{Z}$ este de forma $n\mathbb{Z}$ cu $n \geqslant 0$.*

Demonstraţie. 1) Evident $0 \in n\mathbb{Z}$ pentru orice n. Deci $n\mathbb{Z} \neq \emptyset$. Dacă $x, y \in n\mathbb{Z}$, atunci există $k, l \in \mathbb{Z}$ astfel încît $x = nk$, $y = nl$. Dar atunci $x - y = n(k - l) \in n\mathbb{Z}$ şi deci $n\mathbb{Z}$ este subgrup al lui $\mathbb{Z}$.

3) Fie H un subgrup al lui $\mathbb{Z}$. Dacă $H = \{0\}$, atunci $H = 0\mathbb{Z}$. Dacă $H \neq \{0\}$, există un număr întreg $x \neq 0$, $x \in H$. Cum şi $-x \in H$, atunci în H există un număr întreg pozitiv. Fie n cel mai mic număr întreg > 0 ce aparţine lui H. Vom dovedi că $H = n\mathbb{Z}$. Cum $n \in H$, rezultă că $n\mathbb{Z} \subset H$. Fie acum $y \in H$; atunci există $q, r \in \mathbb{Z}$ astfel încît

$$y = nq + r, \quad 0 \leqslant r < n.$$

Atunci $r = y - nq \in H$, deoarece $y \in H$ şi $nq \in H$. Dar cum

Scanned with OKEN Scanner

n este cel mai mic întreg > 0 ce aparţine lui H, rezultă că $r = 0$. Deci

$$y = nq \in \mathbb{Z} \text{ şi astfel } H \subset n\mathbb{Z}.$$

— *Noţiunea de inel*

Definiţia 5.3. Se numeşte *inel* o mulţime A înzestrată cu două operaţii algebrice: $+ : A \times A \to A$ şi $\cdot : A \times A \to A$, una notată aditiv şi cealaltă multiplicativ, care satisfac următoarele proprietăţi:

1) A este grup abelian faţă de operaţia aditivă;
2) operaţia de înmulţire este asociativă;
3) oricare ar fi $x, y, z \in A$, avem

$$(x + y)z = xz + yz,$$
$$x(y + z) = xy + xz$$

(distributivitatea înmulţirii faţă de adunare).

Într-un inel, operaţia aditivă se mai numeşte *adunare* iar cea multiplicativă *înmulţire.*

În cazul unui inel A, grupul abelian A faţă de adunare se numeşte *grupul aditiv* al inelului. Elementul neutru al acestui grup se notează, de obicei, cu 0 şi se numeşte *elementul zero* al inelului, iar inversul faţă de adunare al unui element oarecare $x \in A$ se notează, de obicei, cu $-x$ şi se mai numeşte *elementul opus* lui x. Astfel, condiţiile 1)—3) se enunţă explicit în modul următor:

1° $x + y = y + x$, oricare ar fi $x, y \in A$;
2° $(x + y) + z = x, + (y + z)$, oricare ar fi $x, y, z \in A$;
3° există un element $0 \in A$ (element zero) astfel încît

$$x + 0 = 0 + x, \text{ oricare ar fi } x \in A;$$

4° pentru orice $x \in A$, există elementul opus lui x, notat $-x \in A$, astfel încît

$$x + (-x) = (-x) + x = 0;$$

5° $x(yz) = (xy)z$, oricare ar fi $x, y, z \in A$;

6° $x(y + z) = xy + xz$ și $(x + y)z = xz + yz$, oricare ar fi $x, y, z \in A$.

Dacă, în plus, operația de înmulțire admite element neutru (unitate), se spune că inelul este *cu element unitate* sau *unitar*. Elementul neutru se notează, de obicei, cu 1. Atunci, inelul este unitar dacă există un element $1 \in A$, astfel încît

$$x1 = 1x = x,$$

oricare ar fi $x \in A$. În acest caz, elementul 1 se numește *element unitate* sau *unitatea* inelului A.

Dacă înmulțirea este comutativă, adică $xy = yx$, pentru orice $x, y \in A$, inelul se numește *comutativ*.

Exemple de inele

1. Mulțimile $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ și $\mathbb{C}$ cu operațiile de adunare și înmulțire sînt inele.

2. Dacă $n \in \mathbb{Z}$ este un număr întreg, atunci $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ este inel față de adunarea și înmulțirea obișnuită a numerelor întregi.

Propoziția 5.4. *Într-un inel A sînt adevărate următoarele afirmații:*

1) $x0 = 0x = 0$, *oricare ar fi* $x \in A$;

2) $(-x)y = x(-y) = -xy$ *și* $(-x)(-y) = xy$, *oricare ar fi* $x, y \in A$.

Demonstrație. 1) Avem $x0 = x(0 + 0) = x0 + x0$. Reducînd $x0$ din ambii membri, rezultă $x0 = 0$. De asemenea, se arată că $0 = 0x$.

2) Avem $0 = 0y = (x + (-x))y = xy + (-x)y$. Deci opusul lui xy este $(-x)y$, de unde $(-x)y = -xy$. La fel se arată că $x(-y) = -xy$. În sfîrșit,

$$(-x)(-y) = -(x(-y)) = -(-xy) = xy.$$

Un *omomorfism* de inele este o aplicație φ de la un inel A într-un alt inel A', astfel încît

$$\varphi(x + y) = \varphi(x) + \varphi(y),$$

$$\varphi(xy) = \varphi(x)\,\varphi(y), \text{ oricare ar fi } x, y \in A.$$

Scanned with OKEN Scanner

Dacă A și A' sînt inele unitare și $\varphi(1) = 1$, atunci omomorfismul se numește *unitar*. Ca și la grupuri, un omomorfism φ de inele se numește *monomorfism*, *epimorfism* sau *izomorfism*, dacă aplicația φ este injectivă, surjectivă sau bijectivă. De exemplu, incluziunile $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sînt monomorfisme de inele. Pentru un inel A funcția identică 1_A este omomorfism de inele.

Definiția 5.4. Un element $x \neq 0$ din inelul comutativ A se numește *divizor al lui zero* dacă există $y \neq 0$, $y \in A$, astfel încît $xy = 0$. Un inel comutativ și unitar cu $1 \neq 0$ și fără divizori ai lui zero se numește *domeniu de integritate*.

Inelul $\mathbb{Z}$ al numerelor întregi este un domeniu de integritate.

Propoziția 5.5. *Un inel A, comutativ și unitar cu $1 \neq 0$, este domeniu de integritate dacă și numai dacă pentru orice $x, y, z \in A$*

$$xy = xz \text{ și } x \neq 0 \Rightarrow y = z.$$

Demonstrație. Fie $x, y \in A$, $x \neq 0$ și $xy = 0$. Atunci $xy = x0$ și din regula de simplificare rezultă $x = 0$. Reciproc, dacă A este un domeniu de integritate, $xy = xz$ și $x \neq 0$ atrage $x(y - z) = 0$ și $x \neq 0$. Deci $y - z = 0$, adică $y = z$.

Definiția 5.5. Fie A un inel. O submulțime nevidă $S \subset A$ se numește *subinel* al lui A dacă S împreună cu operațiile induse de cele de pe A formează la rîndul său un inel.

Propoziția 5.6. *Fie A un inel și $S \subset A$ o submulțime nevidă a lui A. Atunci S este un subinel al lui A dacă și numai dacă:*

1) *oricare ar fi $x, y \in S$, rezultă $x - y \in S$;*
2) *oricare ar fi $x, y \in S$, rezultă $xy \in S$.*

Demonstrație. Cele două condiții asigură că operațiile lui A induc pe S operații algebrice. Faptul că S împreună

cu acestea formează inel este uşor de verificat, deoarece axiomele inelului sînt verificate în inelul A.

Exemple de subinele

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sînt subinele unul în altul faţă de operaţiile de adunare şi înmulţire uzuale.

2. Subinelele lui $\mathbb{Z}$ sînt, evident, de forma $n\mathbb{Z}$, $n \in \mathbb{N}$, adică coincid cu subgrupurile grupului aditiv $\mathbb{Z}$.

— *Noţiunea de corp*

Definiţia 5.6. Un inel unitar K, $1 \neq 0$, se numeşte *corp*, dacă orice element nenul din K este inversabil relativ la înmulţire.

Deci K este corp dacă:

1) K este inel unitar;

2) oricare ar fi $x \in K$, $x \neq 0$, există $x^{-1} \in K$, astfel încît $xx^{-1} = x^{-1}x = 1$.

În plus, dacă înmulţirea este comutativă, se spune că corpul este *comutativ*.

Fie K un corp. Se pun în evidenţă două grupuri şi anume:

1° *grupul aditiv* al lui K, cu alte cuvinte, mulţimea K cu adunarea,

2° *grupul multiplicativ* K^* al elementelor nenule ale lui K.

Aceste două grupuri se numesc *grupuri subiacente* structurii de corp pe K, definite de cele două operaţii.

De exemplu, mulţimile $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$ înzestrate cu operaţiile de adunare şi înmulţire din $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$ respectiv sînt corpuri.

Definiţia 5.7. Dacă inelul K este un corp, o submulţime nevidă F a lui K este un *subcorp* al lui K dacă operaţiile algebrice de pe K induc pe F operaţiile algebrice în raport cu care F este corp.

Scanned with OKEN Scanner

Propoziția 5.7. *Fie K un corp și $F \subset K$ o submulțime a lui K cu cel puțin două elemente. Atunci F este subcorp al lui K dacă și numai dacă:*

1) *oricare ar fi $x, y \in F$, atunci $x - y^{-1} \in F$;*
2) *oricare ar fi $x, y \in F$, $y \neq 0$, atunci $xy^{-1} \in F$.*

Demonstrație. Echivalența celor două afirmații este imediată. Observăm că elementul unitate din K este element unitate pentru F, iar inversul unui element din F este tot în F, după cum rezultă imediat din condiția 2°.

De exemplu, $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sînt subcorpuri unul în altul.

Propoziția 5.8. *Un corp nu are divizori ai lui zero.*

Demonstrație. Fie K un corp și fie, prin absurd, $x \in K$, $x \neq 0$, un divizor al lui zero în K. Atunci există $y \neq 0$, $y \in K$, astfel încît $xy = 0$. Cum $x \neq 0$, există $x^{-1} \in K$. Atunci $x^{-1}xy = 0$ și deci $y = 0$ (contradicție !).

Un *omomorfism* de corpuri este o aplicație φ de la un corp K într-un corp K', astfel încît

$$\varphi(x + y) = \varphi(x) + \varphi(y),$$

$$\varphi(xy) = \varphi(x)\varphi(y), \text{ oricare ar fi } x, y \in K,$$

$$\varphi(1) = 1.$$

Propoziția 5.9. *Fie K și K' două corpuri și $\varphi : K \to K'$ un omomorfism de corpuri.* Atunci:

1) *pentru orice $x \in K$, $x \neq 0$, avem $\varphi(x^{-1}) = (\varphi(x))^{-1}$;*
2) *φ este o aplicație injectivă.*

Demonstrație. 1) rezultă din faptul că φ este un omomorfism de grupuri de la grupul multiplicativ K^* în grupul multiplicativ K'^*.

2) Fie $\varphi(x) = \varphi(y)$, atunci $\varphi(x - y) = 0$. Dacă $x \neq y$, atunci $x - y \neq 0$, deci este inversabil. Fie z inversul său. Din relația $(x - y) \cdot z = 1$ deducem

$$\varphi(x - y)\varphi(z) = \varphi(1) = 1$$

și deci $0 = 1$ (contradicție !).

Scanned with OKEN Scanner

Fie A un inel comutativ și unitar. Se va da în continuare o construcție a inelului de polinoame într-o nedeterminată, peste inelul A care, la început, nu folosește scrierea obișnuită a polinoamelor cu ajutorul unei nedeterminate X.

Fie $A^{(\mathbb{N})}$ mulțimea șirurilor infinite de elemente din A :

$$(a_0, a_1, a_2, \ldots)$$

care *au numai un număr finit de termeni* a_i *nenuli*. Șirurile $(a_0, a_1, a_2, \ldots)$ și $(b_0, b_1, b_2, \ldots)$ sînt *egale* dacă și numai dacă $a_i = b_i$ pentru orice i. Cu alte cuvinte, $A^{(\mathbb{N})}$ este mulțimea funcțiilor f de la mulțimea $\mathbb{N}$ a numerelor naturale în inelul dat A, astfel că $f(i) = 0$ pentru i suficient de mare. Deci o funcție f de la $\mathbb{N}$ în A aparține lui $A^{(\mathbb{N})}$ dacă există un număr natural m, astfel încît $f(i) = 0$, pentru orice $i > m$.

Pe mulțimea $A^{(\mathbb{N})}$ se definesc două operații algebrice, *adunarea și înmulțirea*, în raport cu care $A^{(\mathbb{N})}$ devine un *inel comutativ și unitar*.

Fie $f, g \in A^{(\mathbb{N})}$. Dacă reprezentăm o astfel de funcție din $A^{(\mathbb{N})}$ prin valorile ei, rezultă că se poate scrie

$$f = (a_0, a_1, a_2, \ldots), \; g = (b_0, b_1, b_2, \ldots),$$

unde $f(i) = a_i$ și $g(i) = b_i$, pentru orice i.

Adunarea se definește astfel :

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots).$$

Să observăm că $f + g \in A^{(\mathbb{N})}$. Într-adevăr, dacă $a_i = 0$, pentru orice $i > m$ și $b_j = 0$, pentru orice $j > n$, atunci $a_k + b_k = 0$ pentru orice $k > \max(m, n)$.

Scanned with OKEN Scanner

Este uşor de văzut că $A^{(\mathbb{N})}$ împreună cu adunarea este un *grup abelian*, adică adunarea este asociativă, comutativă, are element nul şi orice element are un opus. Elementul nul (zero) este

$$0 = (0, 0, 0, \ldots),$$

adică funcţia $0 : \mathbb{N} \to A$ astfel încît $0(i) = 0$, oricare ar fi i. Aici avem pe de o parte elementul 0 din A, iar pe de alta elementul 0 din $A^{(\mathbb{N})}$, dar cum se va vedea ulterior, acestea se pot identifica, aşa că folosim acelaşi simbol 0 care să le desemneze.

Dacă $f = (a_0, a_1, a_2, \ldots) \in A^{(\mathbb{N})}$, opusul său este funcţia $f^* : \mathbb{N} \to A$, dată prin $f^*(i) = -a_i$, oricare ar fi i, adică

$$f^* = (-a_0, -a_1, -a_2, \ldots);$$

f^* se notează cu $-f$.

Să definim acum o altă operaţie algebrică pe $A^{(\mathbb{N})}$, anume *înmulţirea*.

Fie $f = (a_0, a_1, a_2, \ldots)$ şi $g = (b_0, b_1, b_2, \ldots)$ două elemente din $A^{(\mathbb{N})}$; atunci

$$fg = (c_0, c_1, c_2, \ldots),$$

unde $c_k = \sum_{i+j=k} a_i b_j$ pentru orice k.

Să observăm că $fg \in A^{(\mathbb{N})}$. Într-adevăr, dacă $a_i = 0$, pentru $i > m$ şi $b_j = 0$, pentru $j > n$, atunci evident $c_k = 0$ pentru $k > m + n$.

Înmulţirea pe $A^{(\mathbb{N})}$ este *asociativă, comutativă şi are element unitate*.

Să demonstrăm asociativitatea. Fie, pentru aceasta, $f, g, h \in A^{(\mathbb{N})}$,

$f = (a_0, a_1, a_2, \ldots)$, $g = (b_0, b_1, b_2, \ldots)$, $h = (c_0, c_1, c_2, \ldots)$

și să arătăm că

$$(fg)h = f(gh).$$

Fie $fg = (d_0, d_1, d_2, \ldots)$. Atunci $d_k = \sum_{i+j=k} a_i b_j$, $(fg)h = (d'_0, d'_1, d'_2, \ldots)$, unde

$$d'_m = \sum_{k+l=m} d_k c_l = \sum_{k+l=m} \left(\sum_{i+j=k} a_i b_j \right) c_l =$$

$$= \sum_{\substack{k+l=m \\ i+j=k}} a_i b_j c_l = \sum_{i+j+l=m} a_i b_j c_l .$$

Fie $gh = (e_0, e_1, e_2, \ldots)$. Atunci

$$e_l = \sum_{i+j=l} b_i c_j \text{ și } f(gh) = (e'_0, e'_1, e'_2, \ldots),$$

unde

$$e'_m = \sum_{k+l=m} a_k e_l = \sum_{k+l=m} a_k \left(\sum_{i+j=l} b_i c_j \right) = \sum_{\substack{k+l=m \\ i+j=l}} a_k b_i c_j = \sum_{i+j+k=m} a_k b_i c_j .$$

Se observă că $d'_m = e'_m$ pentru orice m.

Comutativitatea înmulțirii rezultă din aceeași proprietate a înmulțirii în inelul A și din faptul că în expresia termenilor produsului polinoamelor f și g, termenii factorilor intervin în mod simetric.

Să punem $1 = (1, 0, 0, \ldots)$. Atunci $(a_0, a_1, a_2, \ldots) \times (1, 0, 0, \ldots) = (1, 0, 0, \ldots)(a_0, a_1, a_2, \ldots) = (a_0, a_1, a_2 \ldots)$, deci $(1, 0, 0, \ldots)$ este element unitate. Elementul unitate din $A^{(\mathbb{N})}$ se va identifica pînă la urmă cu elementul unitate al lui A. Acest fapt justifică notația cu același simbol a celor două elemente.

Operația de înmulțire pe $A^{(\mathbb{N})}$ este *distributivă* față de adunare. Într-adevăr, cu notațiile introduse, rezultă

$f(g+h) = (d_0, d_1, d_2, \ldots)$, unde $d_k = \sum_{i+j=k} a_i(b_j + c_j)$;

$fg + fh = (d_0', d_1', d_2', \ldots)$, unde $d_k' = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j$,

şi deoarece operaţia de înmulţire pe A este distributivă faţă de adunare, rezultă

$$f(g+h) = fg + fh.$$

Evident că şi $(f+g)h = fh + gh$.

Aşadar, s-a demonstrat distributivitatea.

În concluzie, $A^{(\mathbb{N})}$ împreună cu cele două operaţii introduse este un inel comutativ şi unitar.

Fie aplicaţia $\varphi : A \to A^{(\mathbb{N})}$, definită prin

$$\varphi(a) = (a, 0, 0, \ldots).$$

Cum $(a, 0, 0, \ldots) = (b, 0, 0, \ldots)$ atrage $a = b$, rezultă că φ este aplicaţie injectivă. De asemenea, relaţiile

$$(a + a', 0, 0, \ldots) = (a, 0, 0, \ldots) + (a', 0, 0, \ldots)$$

şi

$$(aa', 0, 0, \ldots) = (a, 0, 0, \ldots)(a', 0, 0, \ldots),$$

adică

$$\varphi(a + a') = \varphi(a) + \varphi(a') \text{ şi } \varphi(aa') = \varphi(a)\,\varphi(a')$$

dau că φ este un omomorfism de inele. Deci φ este *monomorfism*. Acest lucru ne permite să identificăm elementul a din A cu imaginea sa $\varphi(a) = (a, 0, 0, \ldots)$ din $A^{(\mathbb{N})}$, adică să punem

$$a = (a_0, 0, 0, \ldots) \text{ pentru orice } a \in A.$$

În acest mod A devine un subinel al lui $A^{(\mathbb{N})}$.

Pe de altă parte, notăm $X = (0, 1, 0, \ldots)$. Acest şir particular va fi numit *nedeterminata* X.

Înmulţirea definită ne dă $X^2 = (0, 0, 1, 0, \ldots)$ şi, mai general, pentru orice $i \in \mathbb{N}$

$$X^i = (\underbrace{0, 0, \ldots, 0}_{i \text{ ori}}, 1, 0, \ldots).$$

Utilizînd acum adunarea şi înmulţirea definite pe $A^{(\mathbb{N})}$, se obţine

$$f = (a_0, a_1, a_2, \ldots) = (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) +$$

$$+ (0, 0, a_2, 0, \ldots) + \ldots + (\underbrace{0, 0, \ldots}_{i \text{ ori}}, 0, a_i, 0, \ldots) + \ldots =$$

$$= (a_0, 0, 0, \ldots) + (a_1, 0, 0, \ldots)(0, 1, 0, \ldots) +$$

$$+ (a_2, 0, 0, \ldots)(0, 0, 1, 0, \ldots) + \ldots$$

$$\ldots + (a_i, 0, 0, \ldots)(\underbrace{0, 0, \ldots, 0}_{i \text{ ori}}, 1, 0, \ldots) \ldots =$$

$= a_0 + a_1X + a_2X^2 + \ldots + a_iX^i + \ldots$ (unde există doar un număr finit de termeni nenuli).

Inelul $A^{(\mathbb{N})}$ obţinut se numeşte *inelul polinoamelor în nedeterminata X, cu coeficienţi în inelul A* (sau peste inelul A) şi se notează $A[X]$. Fiecare element al acestui inel se numeşte *polinom*.

$A[X]$ se mai numeşte şi *inelul polinoamelor într-o nedeterminată*.

Fie $f \in A[X]$ un polinom. Să presupunem că toţi $f(i) = a_i = 0$, pentru $i > n$. Atunci f se scrie (evident, în mod unic) sub forma

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n.$$

Fie $A[X]$ inelul polinoamelor într-o nedeterminată cu coeficienţi în inelul A. Atunci pentru un polinom $f \in A[X]$, $f \neq 0$, avem

$$f = \sum_{i=0}^{n} a_i X^i, \qquad a_n \neq 0.$$

Scanned with OKEN Scanner

Se numeşte *gradul lui* f [notat prin $\deg(f)$] cel mai mare număr natural n cu proprietatea $a_n \neq 0$. Atunci polinomul f se scrie sub forma

$$f = \sum_{i=0}^{n} a_i X^i, \text{ unde } a_n \neq 0.$$

În particular, X este un polinom de gradul întîi, X^i este un polinom de grad i şi pentru $a \neq 0$ polinomul $a = (a, 0, 0, \ldots)$ este de gradul zero, numit şi *polinom constant*. Pentru polinomul nul care se notează tot cu 0, gradul său se consideră ca fiind egal cu $-\infty$.

Un polinom $f \in A[X]$ are gradul $\leqslant 0$ dacă şi numai dacă aparţine lui A şi $\deg(f) = 0$ dacă şi numai dacă f este un element nenul al inelului A. Din definiţie rezultă imediat că

$$\deg(f+g) \leqslant \max(\deg(f), \deg(g))$$

şi

$$\deg(fg) \leqslant \deg(f) + \deg(g)$$

pentru orice $f, g \in A[X]$, unde convenim să punem $-\infty < a$, $-\infty + a = -\infty$ şi $(-\infty) + (-\infty) = -\infty$ pentru orice $a \in \mathbb{Z}$.

Mai mult, dacă

$$f = \sum_{i=0}^{m} a_i X^i \text{ şi } g = \sum_{i=0}^{n} b_i X^i$$

cu $a_m \neq 0$, $b_n \neq 0$, iar dacă unul din elementele a_m şi b_n este nondivizor al lui zero în A, atunci

$$\deg(fg) = \deg(f) + \deg(g).$$

Într-adevăr, se observă că polinomul fg are drept coeficient al lui X^{m+n} pe $a_m b_n$ care este diferit de 0 prin ipoteză. Deci $\deg(fg) \geqslant m + n$ şi, cum inegalitatea contrară este evidentă, se obţine egalitate.

Scanned with OKEN Scanner

Inele euclidiene

§ 1. Definiția inelelor euclidiene. Exemple

În cele ce urmează se notează cu A un domeniu de integritate. Deci A este un inel comutativ, unitar (cu $1 \neq 0$) și fără divizori ai lui zero. Avem în vedere inelul $\mathbb{Z}$ al numerelor întregi, inelele $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ ale polinoamelor în nedeterminata X cu coeficienți respectiv întregi, raționali, reali, complecși. Vom studia în particular și inelul $\mathbb{Z}[i]$ *al întregilor lui Gauss*. Elementele inelului $\mathbb{Z}[i]$ sînt numerele complexe $a + ib$ cu a și b numere întregi, operațiile inelului $\mathbb{Z}[i]$ fiind adunarea și înmulțirea obișnuite ale numerelor complexe.

Pe fiecare din inelele enumerate se pot defini funcții cu valori în mulțimea $\mathbb{N}$ a numerelor naturale. Astfel, putem asocia:

— la orice $a \in \mathbb{Z}$, numărul natural $|a|$;

— la orice $a + ib \in \mathbb{Z}[i]$, numărul natural $a^2 + b^2$;

— la orice polinom $f \neq 0$ din $\mathbb{R}[X]$, numărul natural $\deg(f)$.

Noțiunea de inel euclidian, care va fi dată mai jos, valorifică proprietățile numerelor naturale în studiul unor inele cu ajutorul unor funcții cu valori în $\mathbb{N}$, adecvat definite.

Scanned with OKEN Scanner

Definiția 1.1. Un domeniu de integritate A se numește *inel euclidian* dacă există o funcție $\varphi : A \to \mathbb{N}$ cu proprietățile :

1) $\varphi(a) = 0 \Leftrightarrow a = 0$;

2) $\varphi(ab) = \varphi(a)\,\varphi(b)$, oricare ar fi $a, b \in A$;

3) oricare ar fi $a, b \in A$, cu $b \neq 0$, există $q, r \in A$ astfel încît

$$a = bq + r, \qquad \varphi(r) < \varphi(b).$$

Așadar, un inel euclidian este un domeniu de integritate A care poate fi „echipat" cu o funcție $\varphi : A \to \mathbb{N}$ ce satisface 1), 2) și 3) din definiția precedentă.

În continuare, cînd se va afirma că (A, φ) este inel euclidian, trebuie să se înțeleagă că A este domeniu de integritate iar φ o funcție definită pe A și cu valori în $\mathbb{N}$, satisfăcînd 1), 2) și 3) din definiția 1.1.

Proprietatea 3) din definiția 1.1 arată că în inele euclidiene se poate face împărțirea cu rest prin elemente diferite de zero. Elementele q și r din egalitatea $a = bq + r$, cu $\varphi(r) < \varphi(b)$, se numesc respectiv *cîtul* și *restul* împărțirii lui a prin $b \neq 0$.

Propoziția 1.1. *Inelul* $\mathbb{Z}$ *al numerelor întregi este euclidian.*

Demonstrație. Definim funcția $\varphi : \mathbb{Z} \to \mathbb{N}$, prin

$$\varphi(a) = |a|, \text{ oricare ar fi } a \in \mathbb{Z}.$$

Cum $|a| = 0$ dacă și numai dacă $a = 0$, rezultă că φ satisface 1) din definiția 1.1. Pentru orice $a, b \in \mathbb{Z}$ avem

$$\varphi(ab) = |ab| = |a|\,|b| = \varphi(a)\,\varphi(b)$$

și deci φ satisface și 2) din definiția 1.1. Apoi, din teorema 3.6, cap. II rezultă că φ satisface și 3), deci $(\mathbb{Z}, \varphi)$ este inel euclidian.

Propoziția 1.2. *Inelul* $\mathbb{Z}[i]$ *al întregilor lui Gauss este euclidian.*

Scanned with OKEN Scanner

Demonstrație. Dacă $z = \alpha + i\beta$ este un număr complex și $\bar{z} = \alpha - i\beta$ conjugatul lui z, atunci

$$\|z\| \overset{\text{def}}{=} z\bar{z} = (\alpha + i\beta)(\alpha - i\beta) = \alpha^2 + \beta^2$$

se numește *norma* lui z. Se observă că norma unui număr complex este un număr real $\geqslant 0$. Dacă z și z' sînt două numere complexe, atunci $\overline{zz'} = \bar{z}\bar{z}'$, de unde

$$\| zz' \| = zz'\,\overline{zz'} = zz'\,\bar{z}\bar{z}' = z\bar{z}z'\bar{z}' = \| z \|\ \| z' \|.$$

Evident, dacă $z = a + ib \in \mathbb{Z}[i]$, atunci $\| z \| = a^2 + b^2 \in \mathbb{N}$.

Fie $\varphi : \mathbb{Z}[i] \to \mathbb{N}$, $\varphi(z) = \| z \|$, oricare ar fi $z \in \mathbb{Z}[i]$. Din considerațiile precedente rezultă imediat că φ verifică 1) și 2) de la definiția 1.1. Să verificăm acum proprietatea 3). Fie în acest scop $z = a + ib$ și $z' = c + id$, $z' \neq 0$, doi întregi ai lui Gauss. Cum $z' \neq 0$, rezultă că $c^2 + d^2 \neq 0$. Acum din calculul

$$\frac{z}{z'} = \frac{z\bar{z}'}{z'\bar{z}'} = \frac{(ac + bd) + i(bc - ad)}{c^2 + d^2} = \xi + i\eta,$$

unde

$$\xi = \frac{ac + bd}{c^2 + d^2}, \qquad \eta = \frac{bc - ad}{c^2 + d^2},$$

rezultă că

$$z = z'(\xi + i\eta), \qquad \xi,\ \eta \in \mathbb{Q}.$$

Cum orice număr rațional poate fi aproximat cu o eroare $\leqslant 1/2$ de un număr întreg, există $u, v \in \mathbb{Z}$ astfel încît

$$|\xi - u| \leqslant \frac{1}{2}, \qquad |\eta - v| \leqslant \frac{1}{2}.$$

Făcînd notațiile $s = \xi - u$ și $t = \eta - v$, avem

$$s^2 = |\xi - u|^2 \leqslant \frac{1}{4}, \qquad t^2 = |\eta - v|^2 \leqslant \frac{1}{4}.$$

Scanned with OKEN Scanner

De asemenea

$$z = z'(\xi + i\eta) = z'((s + u) + i(t + v)) =$$

$$= z'(u + iv) + z'(s + it).$$

Fie $q = u + iv \in \mathbb{Z}[i]$ și $r = z'(s + it) = z - z'q \in \mathbb{Z}[i]$. Avem

$$\varphi(r) = \| z'(s + it) \| = \| z' \| \| s + it \| =$$

$$= \| z' \| (s^2 + t^2) \leqslant \| z' \| \left(\frac{1}{4} + \frac{1}{4} \right) < \| z' \|,$$

deci

$$z = z'q + r, \qquad \varphi(r) < \varphi(z').$$

Observație. Demonstrația propoziției 1.2 oferă o metodă de împărțire cu rest a întregilor lui Gauss: pentru a împărți z prin $z' \neq 0$, z și z' din $\mathbb{Z}[i]$, se scrie $\frac{z}{z'}$ sub forma $\xi + i\eta$ cu ξ și $\eta \in \mathbb{Q}$ și avem

$$q = u + iv, \qquad r = z - z'(u + iv),$$

unde u și v sînt cele mai bune aproximări întregi ale lui ξ, respectiv η.

Să ilustrăm această metodă în cazul $z = -8 - 5i$ și $z' = 2 + 3i$. Avem

$$\frac{z}{z'} = \frac{-8 - 5i}{2 + 3i} = \frac{(-8 - 5i)(2 - 3i)}{(2 + 3i)(2 - 3i)} = \frac{-31 + 8i}{13} =$$

$$= -\frac{31}{13} + \frac{8}{13} i.$$

Cele mai bune aproximări întregi pentru $\xi = -\frac{31}{13}$ și $\eta = \frac{8}{13}$ sînt $u = -2$, respectiv $v = 1$. Așadar $q = -2 + i$ și $r = -8 - 5i - (2 + 3i)(-2 + i) = -1 - i$. Rezultă

$$-8 - 5i = (2 + 3i)(-2 + i) + (-1 - i)$$

și avem

$$\varphi(r) = (-1 - i)(-1 + i) = 2 < 13 = \varphi(2 + 3i) = \varphi(z').$$

Lema 1.3. *Fie K un corp comutativ, $f,\ g \in K[X]$, $g \neq 0$. Există $q,\ r \in K[X]$ astfel încît*

$$f = gq + r, \qquad \deg(r) < \deg(g).$$

Demonstrație. Dacă $\deg(f) < \deg(g)$, este clar că lema este adevărată luînd $q = 0$ și $r = f$. Rămîne să examinăm cazul $\deg(f) \geqslant \deg(g)$. Fie $m = \deg(f)$, $n = \deg(g)$, $m \geqslant n$ și

$$f = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0, \quad a_m \neq 0,$$

$$g = b_n X^n + b_{n-1} X^{n-1} + \ldots + b_1 X + b_0, \quad b_n \neq 0.$$

Cum K este corp și $b_n \neq 0$, atunci b_n este inversabil în K, deci polinomul de grad m

$$a_m b_n^{-1} X^{m-n} g = a_m X^m + a_m b_n^{-1} b_{n-1} X^{m-1} + \ldots$$

are coeficienții în corpul K. Atunci polinomul

$$f_1 = f - a_m b_n^{-1} X^{m-n} g = (a_{m-1} - a_m b_n^{-1} b_{n-1}) X^{n-1} + \ldots \quad (3.1)$$

este din $K[X]$. Mai mult, $\deg(f_1) \leqslant m - 1$ [avem $\deg(f_1) = m - 1$ dacă și numai dacă $a_{m-1} - a_m b_n^{-1} b_{n-1} \neq 0$]. Presupunînd lema adevărată pentru polinoame de grad $< m$, rezultă că există $q_1,\ r_1 \in K[X]$ astfel încît

$$f_1 = gq_1 + r_1, \ \deg(r_1) < \deg(g).$$

Din (3.1) rezultă

$$f = g(q_1 + a_m b_n^{-1} X^{m-n}) + r_1,$$

și lema este adevărată, luînd $q = q_1 + a_m b_n^{-1} X^{m-n}$ și $r = r_1$.

Observație. Demonstrația lemei precedente motivează din punct de vedere teoretic cunoscutul algoritm al împărțirii cu rest pentru polinoame. Este clar că algoritmul împărțirii cu rest al polinoamelor constă în perfectarea de un număr finit de ori a pasului (3.1), $a_m b_n^{-1} X^{m-n}$ intrînd ca termen al citului la fiecare execuție a pasului (3.1).

Propoziția 1.4. *Pentru orice corp comutativ K, inelul $K[X]$ este euclidian. În particular, inelele de polinoame $\mathbb{Q}[X]$, $\mathbb{R}[X]$ și $\mathbb{C}[X]$ sînt euclidiene.*

Demonstrație. Fie $\varphi : K[X] \to \mathbb{N}$,

$$\varphi(f) = 2^{\deg(f)}, \text{ oricare ar fi } f \in K[X].$$

Cum $\deg(0) = -\infty$ și $\deg(f) \geqslant 0$ pentru $f \neq 0$, rezultă că $\varphi(f) = 0$ dacă și numai dacă $f = 0$. Pentru $f, g \in K[X]$ avem

$$\varphi(fg) = 2^{\deg(fg)} = 2^{\deg(f)+\deg(g)} = 2^{\deg(f)}\, 2^{\deg(g)} = \varphi(f)\, \varphi(g).$$

Rezultă că φ satisface 1) și 2) din definiția 1.1. În sfîrșit, dacă $f, g \in K[X]$ cu $g \neq 0$, din lema 1.3 rezultă că există $q, r \in K[X]$, astfel încît

$$f = gq + r, \quad \deg(r) < \deg(g)$$

și deci $\varphi(r) < \varphi(g)$, de unde rezultă 3).

§ 2. Divizibilitate în domenii de integritate

Fie A un domeniu de integritate. Pentru problematica acestui paragraf A poate fi unul din inelele $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ sau $\mathbb{C}[X]$.

Fie a și b două elemente din A. Spunem că *a divide b* (în inelul A) dacă există $a' \in A$ astfel încît $b = aa'$. Dacă a divide b, scriem $a \mid b$; în caz contrar spunem că *a nu divide b* în inelul A. Cînd a divide b, se mai spune că *b se divide prin a* sau *b este multiplu de a* sau încă *a este divizor al lui b* (în inelul A).

Exemple

1. Dacă $A = \mathbb{Z}$, $a = 3$ și $b = -12$, atunci $a \mid b$ în $\mathbb{Z}$, căci luînd $a' = -4 \in \mathbb{Z}$, avem

$$aa' = 3 \times (-4) = -12 = b.$$

Dacă $a = 2$ și $b = 9$, atunci a nu divide b în inelul $\mathbb{Z}$, căci $2x \neq 9$ oricare ar fi $x \in \mathbb{Z}$ ($2x$ este par pentru orice $x \in \mathbb{Z}$ și 9 este impar). Totuși, luînd $A = \mathbb{Q}$, atunci $2|9$ în $\mathbb{Q}$, căci pentru $a' = 9/2 \in \mathbb{Q}$ avem $aa' = 9$.

2. Dacă $A = \mathbb{Z}[i]$, $a = 1 + i$ și $b = 3 - i$, atunci $a|b$ în inelul $\mathbb{Z}[i]$. Într-adevăr, luînd $a' = 1 - 2i$, avem

$$aa' = (1 + i)(1 - 2i) = 3 - i = b.$$

Dacă $a = 1 + i$ iar $b = 3 = 3 + i \cdot 0$, atunci a nu divide b în inelul $\mathbb{Z}[i]$ căci oricare ar fi $x + iy$ din $\mathbb{Z}[i]$ avem $(1 + i)(x + iy) \neq 3$. Într-adevăr dacă $(1 + i)(x + iy) = 3$ cu $x, y \in \mathbb{Z}$, atunci $x - y = 3$ și $x + y = 0$, de unde $2x = 3$ cu $x \in \mathbb{Z}$, ceea ce nu este posibil.

3. Dacă $A = \mathbb{Z}[X]$, $a = X - 2$ și $b = X^2 - X - 2$, atunci $a|b$ în inelul $\mathbb{Z}[X]$, deoarece luînd $a' = X + 1$, avem

$$aa' = (X - 2)(X + 1) = X^2 - X - 2 = b.$$

Dacă $a = 2X - 4$ și $b = X - 2$, atunci a nu divide b în inelul $\mathbb{Z}[X]$ după cum ușor se poate verifica. Totuși $a|b$ în inelul $\mathbb{Q}[X]$, deoarece luînd $a' = 1/2 \in \mathbb{Q}[X]$, avem

$$aa' = (2X - 4) \cdot \frac{1}{2} = X - 2 = b.$$

Propoziția 2.1. *Relația de divizibilitate pe un domeniu de integritate A are proprietățile:*

1) $a \mid a$, *oricare ar fi* $a \in A$;

2) $a \mid b$ și $b \mid c \Rightarrow a \mid c$;

3) $a \mid b_i, 1 \leqslant i \leqslant n \Rightarrow a \mid \sum_{i=1}^{n} b_i c_i$, *oricare ar fi* $c_i \in A$, $1 \leqslant i \leqslant n$.

Demonstrație. Pentru orice $a \in A$ avem $a \cdot 1 = a$, deci $a \mid a$. Dacă $a \mid b$ și $b \mid c$, atunci $b = aa'$ și $c = bb'$ cu $a', b' \in A$, de unde $c = bb' = a(a'b')$, deci $a \mid c$. În sfîrșit, dacă $a|b_i$, atunci $b_i = aa_i$ cu $a_i \in A$, $1 \leqslant i \leqslant n$. Avem

$$\sum_{i=1}^{n} b_i c_i = \sum_{i=1}^{n} aa_i c_i = a\left(\sum_{i=1}^{n} a_i c_i\right),$$

de unde $a \mid \sum_{i=1}^{n} b_i c_i$. Demonstrația propoziției este terminată.

Scanned with OKEN Scanner

Proprietăţile 1) şi 2) din enunţul propoziţiei 2.1 arată că relaţia de divizibilitate este o relaţie binară pe A reflexivă, respectiv tranzitivă. Proprietatea 3) arată că dacă a divide $b_1, b_2, \ldots, b_n \in A$, atunci a divide orice combinaţie liniară $b_1 c_1 + \ldots + b_n c_n$ de $b_1, \ldots, b_n$ cu coeficienţi $c_1, \ldots, c_n \in A$. Cum $a \cdot 0 = 0$ şi $a \cdot 1 = a$ oricare ar fi $a \in A$, avem $a \mid 0$ şi $1 \mid a$ oricare ar fi $a \in A$.

Un rol special este jucat în teoria divizibilităţii într-un domeniu de integritate A de către divizorii elementului unitate 1 al lui A. Să notăm cu U_A mulţimea tuturor divizorilor în A ai lui $1 \in A$. Este clar că $u \in U_A$ dacă şi numai dacă u este inversabil faţă de înmulţirea inelului A: există $u' \in A$ astfel încît $uu' = 1$. Aşadar

$$u \in U_A \Leftrightarrow u \mid 1 \Leftrightarrow \text{există } u' \in A,\ uu' = 1.$$

Cum $1 \cdot 1 = 1$, rezultă că $1 \in U_A$. Elementele lui U_A se numesc *unităţi ale inelului* A. Este limpede că U_A formează grup faţă de înmulţirea inelului A, numit *grupul unităţilor inelului* A. Propoziţia următoare dă o caracterizare a unităţilor unui inel euclidian.

Propoziţia 2.2. *Dacă* (A, φ) *este un inel euclidian, atunci*

$$U_A = \{u \in A \mid \varphi(u) = 1\}.$$

Demonstraţie. Pentru a evita eventuale confuzii, notăm cu e elementul unitate al lui A pentru a-l distinge de numărul natural 1. Cum $e \neq 0$, avem $\varphi(e) \neq 0$ şi atunci din $\varphi(e) = \varphi(ee) = \varphi(e)\,\varphi(e)$ rezultă că $\varphi(e) = 1$. Dacă $u \in U_A$, fie $u' \in A$ astfel încît $uu' = e$. Avem

$$1 = \varphi(e) = \varphi(uu') = \varphi(u)\,\varphi(u'),$$

de unde $\varphi(u) = 1$.

Reciproc, fie $u \in A$ astfel încît $\varphi(u) = 1$. Făcînd împărţirea cu rest a lui e prin $u \neq 0$, găsim $q, r \in A$, astfel încît

$$e = uq + r, \quad \varphi(r) < \varphi(u).$$

Cum $\varphi(u) = 1$, avem $\varphi(r) = 0$, deci $r = 0$. Rezultă că $e = uq$ cu $q \in A$, de unde $u \in U_A$.

Rezultatul din propoziţia 2.2 poate fi folosit pentru a determina unităţile inelelor euclidiene $\mathbb{Z}$, $\mathbb{Z}[i]$ şi $K[X]$, K fiind corp comutativ. Avem

$$U_{\mathbb{Z}} = \{1, -1\}$$

pentru că 1 şi -1 sînt singurele numere întregi de modul 1. De asemenea

$$U_{\mathbb{Z}[i]} = \{1, -1, i, -i\}.$$

Într-adevăr, fie $z = ib \in \mathbb{Z}[i]$ astfel încît

$$1 = \|z\| = a^2 + b^2.$$

Cum $(1, 0)$, $(-1, 0)$, $(0, 1)$ şi $(0, -1)$ sînt singurele soluţii întregi ale ecuaţiei $X^2 + Y^2 = 1$, rezultă că unităţile inelului $\mathbb{Z}[i]$ sînt 1, -1, i şi $-i$. În sfîrşit, avem

$$U_{K[X]} = K \setminus \{0\}.$$

Cu alte cuvinte, unităţile inelului $K[X]$ sînt polinoamele constante $\alpha \neq 0$, $\alpha \in K$. Într-adevăr, conform propoziţiei 1.4 şi propoziţiei 2.2, avem

$$f \in U_{K[X]} \Leftrightarrow 2^{\deg(f)} = 1 \Leftrightarrow \deg(f) = 0 \Leftrightarrow f = \alpha,\ \alpha \in K,\ \alpha \neq 0.$$

Fie A un domeniu de integritate şi $a, b \in A$. Spunem că *a este asociat în divizibilitate cu b* şi scriem $a \sim b$, dacă $a \mid b$ şi $b \mid a$ în inelul A. Aşadar:

$$a \sim b \Leftrightarrow a \mid b \text{ şi } b \mid a.$$

Relaţia de asociere în divizibilitate este o relaţie de echivalenţă pe A. Într-adevăr, direct din definiţie rezultă că asocierea în divizibilitate este o relaţie binară reflexivă,

Scanned with OKEN Scanner

simetrică și tranzitivă, adică:

1° $a \sim a$, oricare ar fi $a \in A$;

2° $a \sim b \Rightarrow b \sim a$;

3° $a \sim b$ și $b \sim c \Rightarrow a \sim c$.

Următoarea propoziție dă o descriere a elementelor asociate în divizibilitate într-un domeniu de integritate A cu un element dat $a \in A$.

Propoziția 2.3. *Fie A un domeniu de integritate și a, b două elemente din A. Avem*

$$a \sim b \Leftrightarrow b = au,\ u \in U_A.$$

Demonstrație. Presupunem $a \neq 0$ și $b \sim a$. Cum $a \mid b$ și $b \mid a$, avem $b = au$ și $a = bv$ cu $u, v \in A$. Rezultă că $a = auv$, deci $a(1 - uv) = 0$. Cum $a \neq 0$ și inelul A nu are divizori ai lui zero, rezultă $1 - uv = 0$, deci $uv = 1$, de unde $b = au$ cu $u \in U_A$.

Reciproc, dacă $b = au$ cu $u \in U_A$, fie $v \in A$ astfel încît $vu = 1$. Din $b = au$ deducem $bv = auv = a$. Așadar $a \mid b$ și $b \mid a$, de unde $b \sim a$. Dacă $a = 0$, atunci și $b = 0$ și afirmația din enunț este evidentă.

Cum $U_{\mathbb{Z}} = \{1, -1\}$, elementele asociate în divizibilitate cu 12 în inelul $\mathbb{Z}$ sînt $12 \times 1 = 12$ și $12 \times (-1) = -12$.

Cum $U_{\mathbb{Z}[i]} = \{1, -1, i, -i\}$, elementele asociate în divizibilitate cu $3 - 2i$ în inelul $\mathbb{Z}[i]$ sînt

$$3 - 2i,\ -3 + 2i,\ 2 + 3i \text{ și } -2 - 3i.$$

În sfîrșit, cum $U_{\mathbb{Q}[X]} = \mathbb{Q} \setminus \{0\}$, polinoamele asociate în divizibilitate cu $5X^2 + 3X - 7$ în inelul $\mathbb{Q}[X]$ sînt toate polinoamele de forma

$$\alpha(5X^2 + 3X - 7),\ \alpha \in \mathbb{Q},\ \alpha \neq 0.$$

Printre acestea se găsește un singur polinom unitar (polinom cu coeficientul puterii maxime a lui X egal cu 1) și anume cel obținut luînd $\alpha = 5^{-1} = \frac{1}{5}$, deci polinomul

$$X^2 + \frac{3}{5}X - \frac{7}{5}.$$

Propoziția 2.4. *Fie (A, φ) un inel euclidian și $a, b \in A$ astfel încît $a \mid b$ și $b \neq 0$. Atunci:*

1) $\varphi(a) \mid \varphi(b)$ *și în particular* $\varphi(a) \leqslant \varphi(b)$;

2) $\varphi(a) = \varphi(b) \Leftrightarrow a \sim b$;

3) $1 < \varphi(a) < \varphi(b) \Leftrightarrow a \notin U_A$ *și b nu divide a.*

Demonstrație. Cum prin ipoteză $a \mid b$, există $a' \in A$ astfel încît $aa' = b$. Cum $b \neq 0$, rezultă că $a \neq 0$ și $a' \neq 0$ Aplicînd φ egalității $aa' = b$, obținem în $\mathbb{N}$ egalitatea. $\varphi(a)\,\varphi(a') = \varphi(b)$, de unde rezultă 1). Cum $\varphi(b) \neq 0$, avem $\varphi(a) = \varphi(b)$ dacă și numai dacă $\varphi(a') = 1$, ceea ce revine la $a' \in U_A$, adică la $a \sim b$. Afirmația 3) din enunț este acum evidentă.

§ 3. C.m.m.d.c. în inele euclidiene

Fie A un domeniu de integritate iar a și b două elemente din A. Un element $c \in A$ se numește *divizor comun al lui a și b* dacă $c \mid a$ și $c \mid b$. Să notăm cu $D\langle a, b\rangle$ mulțimea divizorilor comuni ai lui a și b. Evident $1 \in D\langle a, b\rangle$ și chiar $U_A \subset D\langle a, b\rangle$, așadar $D\langle a, b\rangle \neq \emptyset$.

Definiția 3.1. Un element $d \in A$ se numește *cel mai mare divizor comun al lui a și b* dacă:

1) $d \in D\langle a, b\rangle$,

2) $c \in D\langle a, b\rangle \Rightarrow c \mid d$.

Scanned with OKEN Scanner

Cu alte cuvinte, d este divizor al lui a şi b şi orice divizor c al lui a şi b este divizor şi al lui d.

Să presupunem că $d' \in A$ satisface de asemenea 1) şi 2) din definiţia precedentă. Cum $d' \in D\langle a, b\rangle$, din proprietatea 2) pentru d rezultă $d' | d$. Analog $d | d'$, deci $d' \sim d$, adică $d' = du$ cu $u \in U_A$.

Aşadar, cel mai mare divizor comun a două elemente a şi b dintr-un domeniu de integritate în caz de există este unic determinat mai puţin o asociere în divizibilitate; făcînd o alegere printre acestea, cel mai mare divizor comun a două elemente a şi b va fi notat cu (a, b).

Observaţie. În $\mathbb{Z}$ numerele asociate în divizibilitate cu $d \in \mathbb{Z}$ $d \neq 0$ sînt d şi $-d$; dintre d şi $-d$ unul şi numai unul este > 0. În $K[X]$, K fiind corp comutativ, polinoamele asociate în divizibilitate cu polinomul $d \in K[X]$, $d \neq 0$,

$$d = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0, \quad a_n \neq 0,$$

sînt αd cu $\alpha \in K$, $\alpha \neq 0$. Dintre aceste, unul şi numai unul este *polinom unitar* (coeficientul lui X^n este 1) şi anume cel care se obţine luînd $\alpha = a_n^{-1}$. Aşadar, punînd condiţia suplimentară de a fi număr pozitiv, respectiv de a fi polinom unitar, cel mai mare divizor comun a două numere întregi, respectiv a două polinoame din $K[X]$ este unic determinat.

Este clar că dacă $a = b = 0$, atunci (a, b) nu poate fi definit ca în definiţia 3.1. Prin definiţie, punem în acest caz $(0, 0) = 0$. Rămîne, lucrînd cu definiţia 3.1, să abordăm problema existenţei lui (a, b) cînd cel puţin unul din elementele a şi b este diferit de zero. Este clar că $(a, b) = a$ cînd $a | b$. În particular, $(a, 0) = a$ cînd $a \neq 0$.

O problemă importantă a teoriei divizibilităţii este desemnarea inelelor A în care (a, b) există, oricare ar fi a şi $b \in A$. Un prim rezultat în acest sens este dat de teorema următoare:

Teorema 3.1. *Fie (A, φ) un inel euclidian. Pentru oricare două elemente $a, b \in A$, (a, b) există. Mai mult, dacă $d = (a, b)$, atunci există $h, k \in A$, astfel încît*

$$d = ah + bk.$$

Demonstrație. Dacă $a = b = 0$, afirmațiile din enunțul teoremei sînt evidente. Considerăm deci cazul în care cel puțin unul din elementele a și b este diferit de zero. Fie

$$I = \{z \in A \mid z = ax + by \text{ cu } x, y \in A\}.$$

Mulțimea I are proprietatea

$$c \in D\langle a, b\rangle \Rightarrow c \mid z, \text{ oricare ar fi } z \in I. \tag{3.2}$$

Într-adevăr, dacă $c \in D\langle a, b\rangle$, există a', $b' \in A$ astfel încît $a = ca'$ și $b = cb'$. Pentru orice $z \in I$ avem

$$z = ax + by = c(a'x) + c(b'y) = c(a'x + b'y),$$

de unde $c \mid z$, oricare ar fi $z \in I$. Luînd $x = 1$ și $y = 0$, obținem $a = a \cdot 1 + b \cdot 0 \in I$ și la fel se arată că $b \in I$. Rezultă, în particular, că I conține elemente diferite de zero și atunci

$$P_{a,b} = \{\varphi(z) \mid z \in I,\ z \neq 0\}$$

este o mulțime nevidă de numere naturale. Fie $d = ah + bk \in I$ astfel încît $\varphi(d)$ este cel mai mic număr natural din $P_{a,b}$. Să arătăm că $d = (a, b)$. Cum $d \in I$, din (3.2) rezultă că d satisface 2) de la definiția 3.1. Să arătăm că d are și proprietatea 1) de la definiția 3.1. Cum $d \neq 0$, există q, $r \in A$ astfel încît

$$a = dq + r, \quad \varphi(r) < \varphi(d).$$

Avem

$$r = a - dq = a - (ah + bk)q = a(1 - hq) + b(-kq) \in I.$$

Dacă $r \neq 0$, atunci $\varphi(r) \in P_{a,b}$ și cum $\varphi(r) < \varphi(d)$, este contrazisă alegerea lui d. Rezultă $r = 0$, deci $a = dq$, de unde $d \mid a$. Analog se arată că $d \mid b$. În definitiv, $d = (a, b)$.

Scanned with OKEN Scanner

Totodată, am obținut și ultima afirmație din enunțul teoremei.

Corolarul 3.2. *Într-un inel euclidian* (A, φ) *avem*

$$(ca, cb) = c(a, b),$$

oricare ar fi $a, b, c \in A$.

Demonstrație. Fie $d = (a, b)$ și fie $h, k \in A$ astfel încît $d = ah + bk$. Este clar că cd divide pe ca și pe cb. Din $cd = cah + cbk$ rezultă că orice divizor al lui ca și al lui cb este divizor și al lui cd, de unde

$$(ca, cb) = cd = c(a, b).$$

Corolarul 3.3. *Fie* (A, φ) *un inel euclidian și* $a, b, c \in A$ *astfel încît* $a \mid bc$ *și* $(a, b) = 1$. *Atunci* $a \mid c$.

Demonstrație. Fie $h, k \in A$ astfel încît $1 = ah + bk$. Avem $c = cah + cbh$. Cum $a \mid ca$ și $a \mid cb$, rezultă că $a \mid (cah + cbk)$, deci $a \mid c$.

Corolarul 3.4. *Fie* (A, φ) *un inel euclidian și* $a, b, c \in A$ *astfel încît* $a \mid c$, $b \mid c$ *și* $(a, b) = 1$. *Atunci* $ab \mid c$.

Demonstrație. Fie $h, k \in A$ astfel încît $1 = ah + bk$. Cum $ab \mid ac$ și $ab \mid bc$, rezultă că ab divide pe $ach + bch = c$.

Definiția 3.2. Fie A un domeniu de integritate și $a, b \in A$. Un element $m \in A$ se numește *cel mai mic multiplu comun al lui* a *și* b dacă:

1) $a \mid m$ și $b \mid m$,

2) $a \mid c$ și $b \mid c \Rightarrow m \mid c$.

Se observă că cel mai mic multiplu comun a două elemente a, b dintr-un domeniu de integritate A este unic determinat mai puțin o asociere în divizibilitate; în caz

Scanned with OKEN Scanner

de există se notează $[a, b]$. Dacă $a = b = 0$, atunci $[0, 0] = 0$. Dacă $a \mid b$, atunci $[a, b] = b$.

Propoziția 3.5. *Fie* (A, φ) *un inel euclidian și* $a, b \in A$. *Atunci* $[a, b]$ *există și*

$$ab = (a, b)[a, b].$$

Demonstrație. Dacă $a = b = 0$, propoziția este evidentă. Presupunem că cel puțin unul din elementele a și b este diferit de zero. Fie $d = (a, b)$ și fie $a', b' \in A$ astfel încît $a = da'$, $b = db'$. Conform corolarului 3.2, avem

$$d = (a, b) = (da', db') = d(a', b'),$$

de unde $(a', b') = 1$. Luînd $m = da'b'$, avem

$$m = ab' = a'b,$$

deci m satisface 1) din definiția 3.2.

Fie $c \in A$ astfel încît $a \mid c$ și $b \mid c$. Fie $x, y \in A$ astfel încît $c = ax = by$. Avem $da'x = db'y$, deci $a'x = b'y$. Folosind corolarul 3.3, rezultă că $a' \mid y$ și $b' \mid x$. Fie $a'', b'' \in A$ astfel încît $y = a'a''$ și $x = b'b''$. Rezultă

$$c = ax = da'b'b'' = mb''$$

și

$$c = by = db'a'a'' = ma''$$

și, în particular, avem $m \mid c$. Așadar, $[a, b]$ există și avem

$$[a, b] = da'b'.$$

În sfîrșit

$$ab = da'db' = (da'b')d = [a, b] \cdot (a, b).$$

Scanned with OKEN Scanner

În paragraful precedent am arătat că într-un inel euclidian (A, φ) pentru orice $a, b \in A$ există $d = (a, b)$ şi mai mult, $d = ah + bk$ cu $h, k \in A$ (vezi teorema 3.1). Demonstraţia teoremei 3.1 este „neconstructivistă", calculul lui d, h, k nu se poate face urmînd ideea acesteia. Într-adevăr, mulţimea

$$P_{a,b} = \{\varphi(z) \mid z = ax + by \neq 0,\ x, y \in A\}$$

este, în afara unor cazuri particulare, infinită.

Ca să găsim pe d, h şi k, trebuie să recunoaştem într-o mulţime infinită $P_{a,b}$ de numere naturale pe cel mai mic. Acest lucru nu este posibil să fie încredinţat, de asemenea, unui calculator electronic, deoarece ar trebui mai întîi să depozităm în memoria acestuia o mulţime infinită de numere naturale, ceea ce din punct de vedere fizic nu este realizabil.

Încă din antichitate este cunoscută o metodă eficientă de calcul al celui mai mare divizor comun pentru două numere naturale, cunoscută sub denumirea de algoritmul lui Euclid. Acest algoritm se transpune imediat în orice inel euclidian (A, φ). Vom regăsi totodată şi rezultatele din teorema 3.1.

Lema 4.1. *Fie A un domeniu de integritate şi $a, b, q, r \in A$ astfel încît*

$$a = bq + r.$$

Avem

1) $D\langle a, b\rangle = D\langle b, r\rangle$;
2) *(a, b) există dacă şi numai dacă (b, r) există şi în acest caz $(a, b) = (b, r)$.*

Demonstraţie. Fie $c \in D\langle b, r\rangle$. Deci $c \mid b$ şi $c \mid r$, de unde rezultă că $c \mid bq + r$, adică $c \mid a$. Deducem că $c \in D\langle a, b\rangle$.

Reciproc, dacă $c \in D\langle a, b\rangle$, atunci c divide pe $a - bq = r$, deci $c \in D\langle b, r\rangle$ și în definitiv $D\langle a, b\rangle = D\langle b, r\rangle$.

Să presupunem că (a, b) există și fie $d = (a, b)$. Cum $D\langle a, b\rangle = D\langle b, r\rangle$, rezultă că $d \mid b$ și $d \mid r$. Dacă $c \in D\langle b, r\rangle$, atunci $c \in D\langle a, b\rangle$, deci $c \mid d$, de unde rezultă că (b, r) există și $(b, r) = d = (a, b)$. La fel se arată că existența lui (b, r) atrage pe acea a lui (a, b) și din nou $(a, b) = (b, r)$.

Fie acum (A, φ) un inel euclidian și $a, b \in A$. Să calculăm pe (a, b). Putem presupune că a nu divide b și b nu divide a [deoarece dacă $a \mid b$, avem $(a, b) = a$ iar dacă $b \mid a$, avem $(a,b) = b$ și calculul lui (a, b) nu ridică probleme]. Putem chiar presupune că $\varphi(b) \leqslant \varphi(a)$. Cum b nu divide pe a, există q_0, $r_0 \in A$ astfel încît

$$a = bq_0 + r_0, \qquad 0 < \varphi(r_0) < \varphi(b).$$

Făcînd acum împărțirea cu rest a lui b prin r_0, avem

$$b = r_0 q_1 + r_1, \qquad \varphi(r_1) < \varphi(r_0).$$

Dacă $r_1 \neq 0$, există q_2, $r_2 \in A$ astfel încît

$$r_0 = r_1 q_2 + r_2, \qquad \varphi(r_2) < \varphi(r_1).$$
$$\cdots\cdots\cdots$$

Dacă $r_{i-1} \neq 0$, există q_i, $r_i \in A$ astfel încît

$$r_{i-2} = r_{i-1} q_i + r_i, \qquad \varphi(r_i) < \varphi(r_{i-1}).$$
$$\cdots\cdots\cdots$$

Observăm că lista împărțirilor succesive poate continua atîta timp cît resturile împărțirii sînt diferite de zero. Afirmăm că există $n \geqslant 0$ astfel încît $r_n \neq 0$ și $r_{n+1} = 0$. Așadar, avem

$$r_{n-2} = r_{n-1} q_n + r_n, \qquad 0 < \varphi(r_n) < \varphi(r_{n-1})$$

și

$$r_{n-1} = r_n q_{n+1} + 0.$$

Într-adevăr, fie

$$P = \{\varphi(r_i) \mid r_i \neq 0, \quad i = 0, 1, 2, \ldots\}.$$

Cum $r_0 \neq 0$, rezultă că P este o mulțime nevidă de numere naturale, deci există n astfel încît $\varphi(r_n)$ este cel mai mic element din P. Cum $r_n \neq 0$, împărțirea cu rest a lui r_{n-1} prin r_n poate fi efectuată, deci

$$r_{n-1} = r_n q_{n+1} + r_{n+1}, \qquad \varphi(r_{n+1}) < \varphi(r_n).$$

Dar $\varphi(r_n)$ fiind cel mai mic număr din P și $\varphi(r_{n+1}) < \varphi(r_n)$, rezultă că $\varphi(r_{n+1}) = 0$, deci $r_{n+1} = 0$.

Observînd că $(r_n, 0)$ există și este egal cu r_n, aplicînd lema 4.1, rezultă succesiv existența pentru

$$(r_{n-1}, r_n), \ (r_{n-2}, r_{n-1}), \ \ldots, (b, r_0), \ (a, b)$$

și mai mult, avem

$$r_n = (r_n, 0) = (r_{n-1}, r_n) = \ldots = (b, r_0) = (a, b).$$

În concluzie, lista de împărțire cu rest, numită *algoritmul lui Euclid* pentru a și b, conduce la un ultim rest diferit de zero, anume r_n, care este chiar cel mai mare divizor comun al elementelor a și b. Astfel am demonstrat:

Teorema 4.2. *Într-un inel euclidian (A, φ) cel mai mare divizor comun a două elemente oarecare $a, b \in A$ există și este egal cu ultimul rest diferit de zero din algoritmul lui Euclid pentru a și b.*

Observații. 1. Rezultatul de la corolarul 3.2 poate fi demonstrat și pe baza teoremei 4.2. Într-adevăr, înmulțind cu $c \neq 0$ toate egalitățile din algoritmul lui Euclid pentru a și b, se obține lista de egalități din algoritmul lui Euclid pentru ca și cb. Cum și ultimul rest diferit de zero se înmulțește cu c, deducem

$$(ca, cb) = c(a, b).$$

2. Într-un inel euclidian (A, φ) algoritmul lui Euclid poate fi folosit și pentru calculul lui $[a, b]$. Într-adevăr, se găsește mai întîi (a, b) cu algoritmul lui Euclid și apoi găsim pe $[a, b]$ din relația $ab = (a, b)\,[a, b]$.

Scanned with OKEN Scanner

3. Se poate extinde în mod natural definiția 3.1 pentru un număr finit $a_1, a_2, \ldots, a_n$ de elemente dintr-un domeniu de integritate A. Cel mai mare divizor comun al elementelor $a_1, a_2, \ldots, a_n$ în caz de există se notează $(a_1, a_2, \ldots, a_n)$. Dacă (A, φ) este inel euclidian, existența și calculul lui $(a_1, a_2, \ldots, a_n)$ sînt asigurate de proprietatea evidentă:

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

Exemple

1. Să calculăm în $\mathbb{Z}$, folosind algoritmul lui Euclid, $(150, -42)$. Cum pentru orice $a, b \in \mathbb{Z}$ avem

$$(a, b) = (-a. b) = (a, -b) = (-a, -b),$$

este suficient să calculăm $(150, 42)$. Avem

$$150 = 42 \times 3 + 24,$$
$$42 = 24 \times 1 + 18,$$
$$24 = 18 \times 1 + 6,$$
$$18 = 6 \times 3 + 0,$$

de unde $(150, -42) = 6$.

2. Să calculăm în inelul $\mathbb{Z}[i]$ al întregilor lui Gauss $(2 + 8i, -3 + i)$. Folosind metoda de împărțire cu rest în $\mathbb{Z}[i]$, expusă în cursul demonstrației propoziției 1.2, avem succesiv:

$$2 + 8i = (-3 + i) \cdot (-2i) + 2i,$$
$$-3 + i = 2i \cdot i + (-1 + i),$$
$$2i = (-1 + i) \cdot (1 - i),$$

de unde

$$(2 + 8i, -3 + i) = -1 + i.$$

3. Fie polinoamele $f = 2X^4 - 3X^3 + 2X^2 - 3X$ și $g = X^3 - X^2 + X - 1$ din $\mathbb{Q}[X]$ și să calculăm (f, g). Folosind algoritmul împărțirii cu rest a polinoamelor, avem

$$2X^4 - 3X^3 + 2X^2 - 3X = (X^3 - X^2 + X - 1)(2X - 1) - X^2 - 1,$$
$$X^3 - X^3 + X - 1 = (-X^2 - 1)(-X + 1),$$

de unde

$$(2X^4 - 3X^3 + 2X^2 - 3X, X^3 - X^2 + X - 1) = X^2 + 1.$$

Scanned with OKEN Scanner

Este cunoscut că pe calculatoare electronice se pot efectua, cu performanţe spectaculoase, procese de calcul numeric dintre cele mai complexe. În realitate, un calculator electronic execută operaţii din cele mai rudimentare: adunarea, scăderea, înmulţirea şi împărţirea numerelor, compararea a două numere etc. numite în continuare *operaţii elementare*. Performanţele calculatoarelor electronice în efectuarea anumitor procese de calcul sînt în esenţă datorate rapidităţii cu care acestea execută operaţiile elementare, precum şi posibilităţii acestora de a executa autonom secvenţe finite de operaţii elementare. Din această cauză, pentru a perfecta pe calculatoare un anumit tip de calcul numeric este necesar ca acesta să fie descompus (cînd este posibil) într-o succesiune finită, bine determinată, de operaţii elementare. Execuţia unei asemenea succesiuni de operaţii elementare se face în conformitate cu o mulţime finită de reguli (instrucţiuni, ordine) care constituie ceea ce se numeşte algoritm al procesului de calcul ce trebuie perfectat. De fapt, algoritmul chiar „produce" secvenţa de operaţii elementare ce urmează să fie efectuate în vederea rezolvării unei probleme specifice de calcul numeric. Am încercat astfel să sugerăm o definiţie pentru conceptul de *algoritm* ca fiind o succesiune finită de instrucţiuni ce conduce, prin producerea şi execuţia unei secvenţe finite de operaţii elementare, la soluţionarea unui tip dat de problemă numerică. Aceasta nu este o definiţie riguroasă a conceptului de algoritm. În realitate, aceasta este o problemă dificilă şi doar parţial rezolvată. Conceptul modern de algoritm este definit în legătură cu maşina Turing, care este un obiect matematic riguros, această definiţie dovedindu-se satisfăcătoare pentru etapa actuală de dezvoltare a ştiinţelor matematice.

Să descriem algoritmi pentru rezolvarea cîtorva tipuri de calcule numerice din aritmetică. Pentru o problemă restrînsă ca aceasta, definiţia vagă a noţiunii de algoritm dată mai sus este suficientă. Pentru a fi comunicat altor persoane, un algoritm poate fi descris verbal, sub forma

Scanned with OKEN Scanner

unei liste finite de instrucţiuni (ordine). Un algoritm poate fi prezentat şi cu mijloace grafice, o asemenea redactare a unui algoritm numindu-se *schemă logică* sau *organigramă*. Menţionăm încă importanta problemă a redactării unui algoritm într-un limbaj pe înţelesul unui calculator electronic dat. Acest lucru se face într-un limbaj de programare (FORTRAN, ALGOL, COBOL etc.) şi prin compilare se obţine algoritmul pentru maşină sau program. Acest lucru nu face obiectul prezentei cărţi.

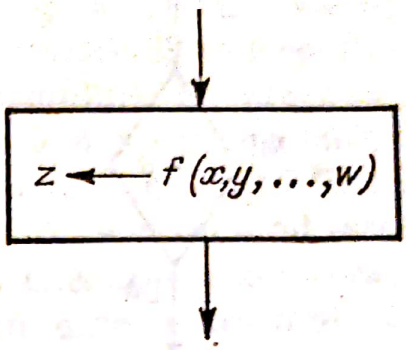


Fig. 3. Bloc de calcul-atribuire.

Se va numi *variabilă* în raport cu un algoritm dat o cantitate susceptibilă de a lua mai multe valori în timpul executării acestuia. Vom nota cu x, y, z, ... variabilele unui algoritm.

În algoritmii elaboraţi pentru efectuarea calculelor numerice cel mai frecvent apare instrucţiunea (ordinul, pasul) de calcul-atribuire, consemnată grafic ca în fig. 3 şi numită bloc de calcul-atribuire. Această instrucţiune trebuie executată astfel: asupra valorilor pe care le au variabilele x, y, ..., w în momentul efectuării acestui pas al algoritmului se face calculul prescris de funcţia f şi valoarea găsită se atribuie variabilei z. Astfel, dacă $f = xy + y^2$, $x = 2$ şi $y = -3$, după executarea instrucţiunii de calcul-atribuire

$$z \leftarrow f(x, y)$$

variabila z va avea valoarea $f(2, -3) = 3$. Dacă $f = x \pmod y$, adică f este egal cu restul împărţirii lui x prin y, şi $x = 14$, $y = 6$, atunci z va lua valoarea $f(14, 6) = 14 \pmod 6 = 2$.

Pentru descrierea unui algoritm sînt folosite şi instrucţiuni care prevăd luarea unei decizii asupra secvenţei de operaţii elementare ce urmează să fie executate în etapa următoare, în funcţie de rezultatul logic al comparării a două numere. O asemenea instrucţiune, grafic, poate fi reprezentată ca în fig. 4 şi se numeşte *bloc de decizie logică*.

Dacă condiţia înscrisă în interiorul blocului de decizie logică este adevărată (are valoarea logică DA), procesul de calcul continuă cu secvenţa de operaţii indicată de

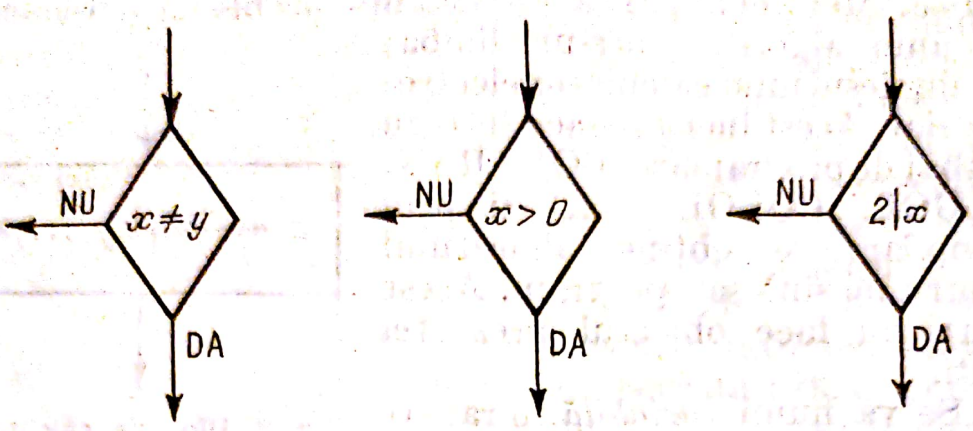


Fig. 4. Blocuri de decizie logică.

săgeata DA; în caz contrar se continuă cu secvenţa de operaţii indicată de săgeata NU.

În prima parte a algoritmului se introduce o instrucţiune care prevede atribuirea valorilor iniţiale a, b, ... unor variabile x, y, ... (intrările algoritmului), ceea ce grafic se desemnează printr-un bloc de iniţializare (vezi fig. 5).

Pentru a consemna în schema logică a algoritmului

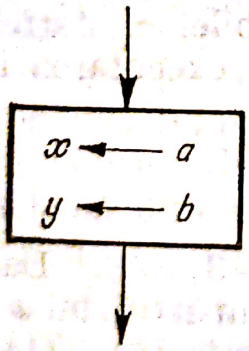


Fig. 5. Bloc de iniţializare.

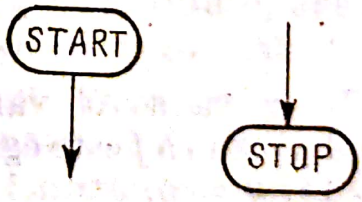


Fig. 6.

începutul şi sfîrşitul acestuia, se folosesc blocurile START, respectiv STOP (vezi fig. 6).

Să exemplificăm cele de mai sus pe algoritmul lui Euclid (vezi § 4). Consideraţiile teoretice făcute în § 4 pot fi

asimilate cu etapa de elaborare a unui algoritm pentru calculul celui mai mare divizor comun a două numere naturale (tipul de calcul numeric). Să redactăm sub forma unei liste de instrucţiuni algoritmul găsit (algoritmul lui Euclid). Introducem trei variabile x, y, z care iau valori numere naturale şi notăm cu d cel mai mare divizor comun ce urmează a fi găsit (ieşirea algoritmului). Să presupunem că trebuie găsit (a, b), unde a şi b sînt numere naturale, $a \geqslant b > 0$. Instrucţiunile se execută una după alta, în ordinea în care apar în listă (în afară de cazul cînd este indicată o schimbare în ordinea de execuţie a acestora) pînă la epuizarea listei, moment în care algoritmul se termină.

Putem redacta algoritmul lui Euclid pentru a şi b astfel :

E_1. Atribuie lui x valoarea a şi lui y valoarea b.

E_2. Calculează restul împărţirii lui x prin y şi atribuie valoarea găsită variabilei z.

E_3. Compară pe z cu 0. Dacă $z = 0$, treci la instrucţiunea E_5.

E_4. Atribuie lui x valoarea y şi apoi lui y valoarea lui z. Treci la instrucţiunea E_2.

E_5. Atribuie lui d valoarea lui y.

Din analiza făcută în § 4, deducem că după un număr finit de paşi se obţine $z = 0$. În etapa următoare se execută instrucţiunea E_5 care dă valoarea lui $d = (a, b)$.

Acelaşi algoritm poate fi descris cu procedee grafice ca în fig. 7. Sensul în care este derulat algoritmul este indicat în schema logică prin săgeţi. Cum în algoritmul lui Euclid executarea succesivă a împărţirilor cu rest conduce după un număr finit de paşi la un rest $= 0$ (vezi § 4),aceasta se traduce prin faptul că secvenţa $E_2E_3E_4$ este parcursă de un număr finit de ori, după care din blocul de decizie E_3 se iese prin săgeata NU şi algoritmul se termină în etapa următoare. În tabelul 1 sînt date valo-

Scanned with OKEN Scanner

rile x, y, z pe măsură ce este derulat algoritmul lui Euclid pentru $a = 150$ și $b = 42$ (vezi exemplul 1, § 4).

x	y	z
150	42	24
42	24	18
24	18	6
18	6	0

Tabelul 1

Dacă (A, φ) este un inel euclidian $a, b \in A$ și $d = (a, b)$, atunci există $h, k \in A$ astfel încît $d = ah + bk$ (vezi teo-

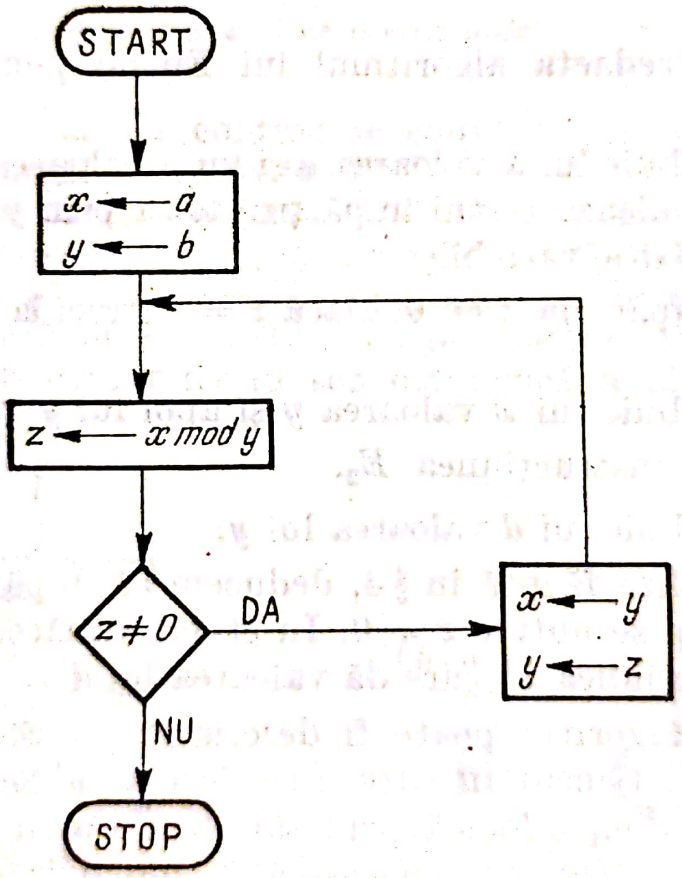


Fig. 7. Schema logică a algoritmului lui Euclid.

rema 3.1). Am văzut că algoritmul lui Euclid dă o metodă de calcul pentru d. În multe situații este necesar să găsim și elementele $h, k \in A$ astfel încît $d = ah + bk$ (vezi cap. V, § 3). Se va expune în continuare un algoritm care con-

duce la găsirea simultană a lui d, h şi k, cunoscut sub denumirea de *algoritmul lui Euclid extins*. Vom prezenta acest algoritm pentru inelul $\mathbb{Z}$.

Fie $a, b \in \mathbb{Z}$, $a > b > 0$. Dacă α este un număr real, notăm cu $[\alpha]$ cel mai mare număr întreg $\leqslant \alpha$; $[\alpha]$ este numit *partea întreagă* a lui α şi

$$\alpha = [\alpha] + \varepsilon, \quad 0 \leqslant \varepsilon < 1.$$

Să considerăm lista împărţirilor succesive din algoritmul lui Euclid pentru a şi b :

$$\begin{aligned} a &= bq_0 + r_0, & r_0 &< b, \\ b &= r_0 q_1 + r_1, & r_1 &< r_0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{i-2} &= r_{i-1} q_i + r_i, & r_i &< r_{i-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Observăm că

$$r_0 = ah_0 + bk_0,$$

unde

$$h_0 = 1, \; k_0 = -q_0 = -\left[\frac{a}{b}\right],$$

şi

$$r_1 = ah_1 + bk_1,$$

unde

$$h_1 = -q_1 = -\left[\frac{b}{r_0}\right], \quad k_1 = 1 + q_0 q_1.$$

Presupunem că $i \geqslant 2$ şi că există h_{i-2}, h_{i-1}, k_{i-2} şi k_{i-1} din $\mathbb{Z}$ astfel încît

$$r_{i-2} = ah_{i-2} + bk_{i-2}, \quad r_{i-1} = ah_{i-1} + bk_{i-1}.$$

Rezultă

$$r_i = r_{i-2} - r_{i-1}q_i = ah_{i-2} + bk_{i-2} - (ah_{i-1} + bk_{i-1})q_i =$$
$$= a(h_{i-2} - h_{i-1}q_i) + b(k_{i-2} - k_{i-1}q_i),$$

deci

$$r_i = ah_i + bk_i, \quad h_i, k_i \in \mathbb{Z}, \tag{3.3}$$

unde

$$h_i = h_{i-2} - h_{i-1}q_i, \quad k_i = k_{i-2} - k_{i-1}q_i$$

cu $q_i = \left[\frac{r_{i-2}}{r_{i-1}}\right]$.

S-a demonstrat astfel, prin inducție asupra lui i, că relația (3.3) se verifică pentru orice $i \geqslant 0$ astfel încît $r_i \neq 0$.

Se observă că

$$(h_i, k_i, r_i) = (h_{i-2}, k_{i-2}, r_{i-2}) - (h_{i-1}, k_{i-1}, r_{i-1})q_i, \tag{3.4}$$

unde $q_i = \left[\frac{r_{i-2}}{r_{i-1}}\right]$ pentru orice $i \geqslant 2$ cu $r_i \neq 0$,

$$(h_{-2}, k_{-2}, r_{-2}) = (1, 0, a)$$

și

$$(h_{-1}, k_{-1}, r_{-1}) = (0, 1, b).$$

Rezultă că (3.3) este adevărat pentru orice $i \geqslant -2$ și (3.4) este adevărat pentru orice $i \geqslant 0$ cu $r_i \neq 0$. În sfîrșit, să observăm că h, k și d căutați sînt respectiv egali cu h_n, k_n, r_n, unde n este unicul număr natural astfel încît $r_n \neq 0$ și $r_{n+1} = 0$.

Pentru formularea algoritmului căutat se introduc variabilele u, v, x, s, t, y, ξ, η, z, q. Pentru $a, b \in \mathbb{Z}$, $a > b > 0$ dați, fie d, h, k numerele întregi cu proprietățile $d = (a, b)$ și $d = ah + bk$. Analiza făcută motivează din punct de vedere teoretic următorul algoritm de calcul

al lui d, h, k, numit *algoritmul lui Euclid extins pentru a și b.*

A_1. $(u, v, x) \leftarrow (1, 0, a)$, $(s, t, y) \leftarrow (0, 1, b)$.

A_2. $z \leftarrow x \bmod y$.

A_3. Dacă $z = 0$, treci la instrucțiunea A_6.

A_4. $q \leftarrow [x/y]$, $(\xi, \eta, z) \leftarrow (u, v, x) - (s, t, y)q$.

A_5. $(u, v, x) \leftarrow (s, t, y)$ și apoi $(s, t, y) \leftarrow (\xi, \eta, z)$. Treci la instrucțiunea A_3.

A_6. $(h, k, d) \leftarrow (s, t, y)$.

Schema logică a algoritmului lui Euclid extins este fig. 8. O instrucțiune de forma

$$(x, y, z) \leftarrow (a, b, c)$$

trebuie interpretată astfel: atribuie lui x valoarea a, lui y valoarea b și lui z valoarea c.

Să observăm că variabilele x, y, z au în algoritmul lui Euclid și în algoritmul lui Euclid extins aceleași valori. Acest lucru se observă și în tabelul 2 care dă valorile variabilelor din algoritmul lui Euclid extins pentru $a = 150$ și $b = 42$ (vezi și tabelul 1).

q	u	v	x	s	t	y	z
	1	0	150	0	1	42	24
3	0	1	42	1	−3	24	18
1	1	−3	24	−1	4	18	6
1	−1	4	18	2	−7	6	0

Tabelul 2

Pentru acest caz avem $h=2$, $k=-7$, $d=6$ și $6=150\times 2+42\times(-7)$

§ 6. Sisteme de numerație

Necesitatea practică de a opera cu multe numere face ineficientă încercarea de a repera fiecare număr cu o „etichetă" fără nici o legătură cu cele afectate celorlalte

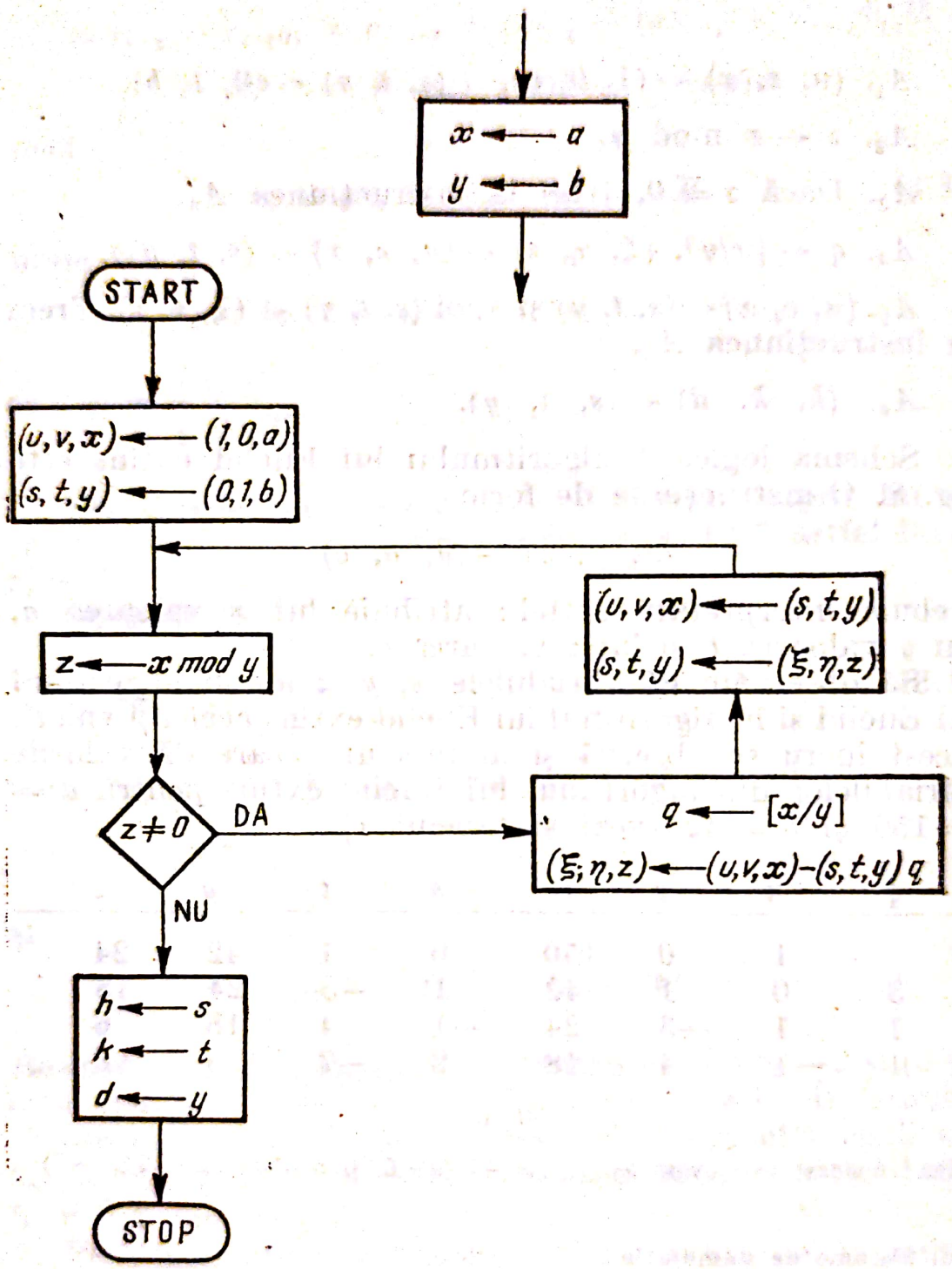


Fig. 8. Schema logică a algoritmului lui Euclid extins.

numere. Din cele mai vechi timpuri s-a impus găsirea unor procedee de scriere a numerelor care să permită o rapidă estimare a ordinului lor de mărime precum şi elaborarea unor reguli simple de a efectua principalele operaţii cu acestea (adunarea, scăderea, înmulţirea, împărţirea). Acestei probleme i s-au dat rezolvări specifice diferitelor etape străbătute de către omenire. Adoptarea sistemului de numeraţie zecimal, cu care sîntem obişnuiţi, s-a încheiat abia în secolele XVI—XVII, cînd acesta a cunoscut o largă răspîndire în Europa, şi reprezintă o importantă etapă în dezvoltarea matematicii.

Reprezentarea numerelor în sistemul de numeraţie în bază u, unde u este un număr natural > 1, se argumentează teoretic prin rezultatul din teorema 6.3.

Lema 6.1. *Fie u un număr natural > 1. Oricare ar fi numărul natural $a > 0$, există numerele naturale n, q_0, q_1, ..., q_{n-1}, a_0, a_1, ..., a_n astfel încît*

$$a = uq_0 + a_0, \quad 0 \leqslant a_0 < u,$$

$$q_0 = uq_1 + a_1, \quad 0 \leqslant a_1 < u,$$

$$\cdots\cdots\cdots$$

$$q_{n-2} = uq_{n-1} + a_{n-1}, \quad 0 \leqslant a_{n-1} < u,$$

$$q_{n-1} = a_n \quad 0 < a_n < u.$$

Demonstraţie. Dacă $a < u$, luăm $n = 0$, $a_0 = a$ şi lema este adevărată. Dacă $a \geqslant u$, fie q_0, $a_0 \in \mathbb{N}$ astfel încît

$$a = uq_0 + a_0, \quad 0 \leqslant a_0 < u.$$

Cum $a \geqslant u$, avem $q_0 > 0$. Există q_1, $a_1 \in \mathbb{N}$ astfel încît

$$q_0 = uq_1 + a_1, \quad 0 \leqslant a_1 < u,$$

şi aşa mai departe.

Dacă $q_i \neq 0$, atunci din $1 < u$ rezultă

$$q_i < uq_i \leqslant uq_i + a_i = q_{i-1},$$

de unde

$$a > q_0 > q_1 > \ldots > q_{i-1} > q_i > \ldots \geqslant 0.$$

Este clar că există n astfel încît $q_{n-1} \neq 0$ și $q_n = 0$. Rezultă că

$$0 < q_{n-1} = a_n < u$$

și lema este demonstrată.

Lema 6.2. *Fie* $u, a_0, a_1, \ldots, a_n \in \mathbb{N}$ *astfel încît* $u > 1, 0 \leqslant a_i < u$ *pentru* $0 \leqslant i < n$ *și* $0 < a_n < u$. *Atunci*

$$\sum_{i=0}^{n} a_i u^i < u^{n+1}.$$

Demonstrație. Cum $a_i \leqslant u - 1$ pentru $i = 0, 1, \ldots, n$, atunci

$$\sum_{i=0}^{n} a_i u^i \leqslant \sum_{i=0}^{n} (u-1)u^i = u^{n+1} - 1 < u^{n+1},$$

de unde rezultă lema.

Teorema 6.3. *Fie* u *un număr natural* > 1. *Oricare ar fi numărul* $a > 0$, *există numerele naturale* $n, a_n, a_{n-1}, \ldots, a_0$ *unic determinate astfel încît*

$$a = a_n u^n + a_{n-1} u^{n-1} + \ldots + a_1 u + a_0,$$

unde $0 < a_n < u$ *și* $0 \leqslant a_i < u$ *pentru* $0 \leqslant i \leqslant n - 1$.

Demonstrație. Conform lemei 6.1, există $n, q_0, \ldots, q_{n-1}$ și $a_0, a_1, \ldots, a_n$ astfel încît

$$\begin{aligned}
a &= uq_0 + a_0, \quad 0 \leqslant a_0 < u, \\
q_0 &= uq_1 + a_1, \quad 0 \leqslant a_1 < u, \\
&\ldots\ldots\ldots \\
q_{n-2} &= uq_{n-1} + a_{n-1}, \quad 0 \leqslant a_{n-1} < u, \\
q_{n-1} &= a_n, \quad 0 < a_n < u.
\end{aligned}$$

Scanned with OKEN Scanner

Înmulțim aceste egalități respectiv cu $1, u, u^2, \ldots, u^n$. Adunînd apoi termen cu termen egalitățile ce se obțin, rezultă

$$a = a_n u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0.$$

Rămîne să dovedim unicitatea numerelor $n, a_n, a_{n-1}, \ldots, a_1, a_0$. Fie de asemenea numerele naturale $n', a'_{n'}, a'_{n'-1}, \ldots, a'_1, a'_0$ astfel încît

$$a = a'_{n'}u^{n'} + a'_{n'-1}u^{n'-1} + \ldots + a'_1 u + a'_0$$

cu $0 < a'_{n'} < u$ și $0 \leqslant a'_i < u$ pentru $0 \leqslant i < n'$.

Dacă $n < n'$, atunci $n + 1 \leqslant n'$ și din lema 6.2 rezultă

$$a = \sum_{i=1}^{n} a_i u^i < u^{n+1} \leqslant u^{n'} \leqslant \sum_{i=0}^{n'} a'_i u^i = a,$$

deci $a < a$ (contradicție). Analog, se arată că nu este posibil ca $n' < n$, de unde $n = n'$.

Să demonstrăm acum că $a_i = a'_i$, $0 \leqslant i \leqslant n$. Dacă $n = 0$, atunci $a_0 = a = a'_0$. Presupunem că $n > 0$ și că afirmația este adevărată pentru $n - 1$. Din egalitățile

$$a = a_0 + u(a_n u^{n-1} + \ldots + a_1) =$$
$$= a'_0 + u(a'_n u^{n-1} + \ldots + a'_1),$$

unde $0 \leqslant a_0 < u$ și $0 \leqslant a'_0 < u$, rezultă, folosind unicitatea cîtului și restului împărțirii lui a prin u (vezi teorema 3.6, cap. II)

$$a_0 = a'_0$$

și

$$a_n u^{n-1} + \ldots + a_2 u + a_1 = a'_n u^{n-1} + \ldots + a'_2 u + a'_1.$$

Folosind ipoteza inducției, din ultima egalitate deducem că

$$a_i = a'_i, \quad i = 1, 2, \ldots, n.$$

Teorema este astfel complet demonstrată.

Sîntem acum în măsură să definim ceea ce este cunoscut sub numele de *sistem de numerație în bază u*, unde u este un număr natural > 1.

La fiecare număr natural $a > 0$ facem să corespundă secvența finită de numere naturale

$$a_n a_{n-1} \ldots a_1 a_0,$$

unde $a_i < u$, $0 \leqslant i \leqslant n$, $a_n \neq 0$, și

$$a = \sum_{i=0}^{n} a_i u^i.$$

Așadar,

$$a_n a_{n-1} \ldots a_1 a_0 \overset{\text{def}}{=} a_n u^n + a_{n-1} u^{n-1} + \ldots + a_1 u + a_0.$$

Din teorema 6.3 rezultă că se stabilește astfel o corespondență biunivocă între numerele naturale > 0 și secvențele finite $a_n a_{n-1} \ldots a_1 a_0$ de numere naturale $a_i < u$, cu $a_n \neq 0$. Cînd se impune să atragem atenția asupra bazei sistemului de numerație, se obișnuiește să se scrie încă $a_n a_{n-1} \ldots a_1 a_{0(u)}$.

Dacă baza sistemului de numerație este u, atunci numerele naturale $c < u$ se numesc *cifrele sistemului de numerație*.

Cel mai răspîndit sistem de numerație este cel în bază zece (notată cu 10) numit *sistemul zecimal*. Cifrele sistemului zecimal de numerație se numesc *cifre zecimale*. Ele sînt numerele naturale mai mici ca zece și se notează în ordine cu

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

Secvența de cifre zecimale 75038 sau mai precis $75038_{(10)}$ reprezintă, așadar, numărul natural

$$7 \times 10^4 + 5 \times 10^3 + 0 \times 10^2 + 3 \times 10 + 8.$$

Dacă $u = 2$, atunci avem *sistemul de numerație binar*, cifrele binare fiind 0 și 1. Astfel:

$$11010_{(2)} = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 0 = 26_{(10)}.$$

Printre sistemele de numerație mai des folosite se numără și cel de bază $u = 16_{(10)} = 10000_{(2)}$ numit *sistemul de numerație hexagesimal*, cifrele hexagesimale fiind

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, E, F.$$

Astfel, avem

$$27_{(10)} = 1A_{(16)} = 11011_{(2)}.$$

Iată o listă de probleme care se pun în mod natural în legătură cu reprezentarea numerelor într-o bază.

(I) Stabilirea raportului de mărime între două numere reprezentate în aceeași bază.

(II) Stabilirea unor reguli (algoritmi) de efectuare a sumei, produsului etc. a două numere reprezentate în aceeași bază.

(III) Elaborarea unor algoritmi pentru reprezentarea unui număr într-o bază dată.

Se va arăta în continuare cum pot fi soluționate aceste probleme pentru numere naturale.

În teorema următoare se dă un criteriu foarte comod de a stabili raportul de mărime între două numere naturale reprezentate în aceeași bază.

Teorema 5.4. *Fie a și b două numere naturale, $a = a_m a_{m-1} \ldots a_1 a_{0(u)}$ și $b = b_n b_{n-1} \ldots b_1 b_{0(u)}$. Atunci $a < b$ dacă și numai dacă $m < n$ sau $m = n$ și $a_p < b_p$, unde p este cel mai mare i astfel încît $a_i \neq b_i$.*

Demonstrație. Dacă $m < n$, din lema 6.2 rezultă $a < u^{m+1} \leqslant u^n \leqslant b$, deci $a < b$. Dacă $m = n$ și $a_p < b_p$,

unde $p = \max \{i \mid a_i \neq b_i\}$, atunci

$$b - a = (b_p - a_p)u^p + (b_{p-1}u^{p-1} + \ldots + b_0) -$$
$$- (a_{p-1}u^{p-1} + \ldots + a_0) > (b_p - a_p)u^p + (b_{p-1}u^{p-1} + \ldots$$
$$\ldots + b_0) - u^p \geqslant u^p + (b_{p-1}u^{p-1} + \ldots + b_0) - u^p \geqslant 0,$$

de unde $b - a > 0$, deci $a < b$.

Reciproc, presupunem că $a < b$. Atunci $m \leqslant n$, deoarece $m > n$ implică $b < a$. Dacă $m < n$, nu mai avem nimic de demonstrat. Dacă $m = n$, fie $p = \max \{i \mid a_i \neq \neq b_i\}$. Avem $a_p < b_p$, întrucît $a_p > b_p$ implică, conform primei părţi a demonstraţiei, $b < a$. Teorema este demonstrată.

Astfel, pentru numerele 125302 şi 95034 date în baza zece avem 125302>95034. La fel, pentru numerele 101101 şi 100110 date în baza doi avem 101101>100110.

Referitor la problema II se va arăta cum se face adunarea şi înmulţirea numerelor naturale reprezentate într-o bază u. În particular, dacă $u = 10$, se regăsesc cunoscutele procedee de adunare şi înmulţire a numerelor naturale.

Fie a, b două numere naturale, $a = a_m a_{m+1} \ldots a_1 a_{0(u)}$, $b = b_n b_{n-1} \ldots b_1 b_{0(u)}$. Trebuie să găsim cifrele c_0, c_1, ... ale numărului $a + b$ în bază u. Putem scrie

$$a = a_0 + a_1 u + a_2 u^2 \ldots$$

şi

$$b = b_0 + b_1 u + b_2 u^2 + \ldots$$

Cum $a_0 < u$ şi $b_0 < u$, rezultă că $a_0 + b_0 < 2u$, deci

$$a_0 + b_0 = u\varepsilon_1 + c_0, \quad 0 \leqslant c_0 < u, \quad \varepsilon_1 = 0 \text{ sau } \varepsilon_1 = 1;$$

mai precis, avem $\varepsilon_1 = 0$ şi $c_0 = a_0 + b_0$ dacă $a_0 + b_0 < u$ iar $\varepsilon_1 = 1$ şi $c_0 = a_0 + b_0 - u$ dacă $u \leqslant a_0 + b_0 < 2u$. Rezultă

$$a + b = c_0 + (a_1 + b_1 + \varepsilon_1)u + (a_2 + b_2)u^2 + \ldots$$

Scanned with OKEN Scanner

Evident, $a_1 + b_1 + \varepsilon_1 < 2u$, de unde

$$a_1 + b_1 + \varepsilon_1 = u\,\varepsilon_2 + c_1, \quad 0 \leqslant c_1 < u,$$

unde $\varepsilon_2 = 0$ sau $\varepsilon_2 = 1$. Avem

$$a + b = c_0 + c_1 u + (a_2 + b_2 + \varepsilon_2)u^2 + \ldots$$

ş.a.m.d.

Se deduce că cifrele $c_0, c_1, c_2, \ldots$ ale sumei $a + b$ sînt:

$$c_i = (a_i + b_i + \varepsilon_i) \bmod u, \quad i = 0, 1, 2, \ldots$$

unde $\varepsilon_0 = 0$, şi pentru $i > 0$:

$\varepsilon_i = 0 \Leftrightarrow a_{i-1} + b_{i-1} + \varepsilon_{i-1} < u$ şi atunci $c_{i-1} = a_{i-1} + b_{i-1} + \varepsilon_{i-1}$,

$\varepsilon_i = 1 \Leftrightarrow a_{i-1} + b_{i-1} + \varepsilon_{i-1} \geqslant u$ şi atunci $c_{i-1} = a_{i-1} + b_{i-1} + \varepsilon_{i-1} - u$.

Cînd $m = n$, numărul $a + b$ are:

1) m cifre dacă $a_n + b_n + \varepsilon_n < u$,

2) $m + 1$ cifre dacă $a_n + b_n + \varepsilon_n \geqslant u$, cifra de rang $m + 1$ fiind în acest caz $c_{m+1} = 1$.

Dacă $m \neq n$, de exemplu $m > n$, atunci cele de mai înainte rămîn adevărate luînd $b_{n+1} = \ldots = b_m = 0$.

Se observă că pentru a efectua $a + b$ în baza u mai trebuie să cunoaştem, sau să avem posibilitatea să consultăm, tabla adunării numerelor naturale $< u$. De exemplu, dacă $u = 5$, tabla adunării numerelor naturale < 5, cu rezultatele exprimate în baza 5, este cea din tabelul 3. În acest tabel la intersecţia liniei numărului i cu coloana numărului j este pus $i + j$ reprezentat în baza 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

Tabelul 3. Tabla adunării în baza 5

Cititorul poate singur acum să redacteze un algoritm al adunării numerelor naturale în baza u, luînd ca motivație teoretică a acestuia considerațiile de mai sus. Observăm că în acest algoritm apare variabila ε care are valoarea inițială $\varepsilon_0 = 0$ iar valorile ε_i, $i \geqslant 1$, sînt egale cu 1 cînd $a_{i-1} + b_{i-1} + \varepsilon_{i-1} \geqslant u$, respectiv 0 cînd $a_{i-1} + b_{i-1} + \varepsilon_{i-1} < u$. Se spune că variabila ε realizează transportul unității de la cifrele de rang i la cele de rang $i + 1$, $i = 0, 1, \ldots$

În calculul cu „creionul și hîrtia" al sumei a două numere naturale, operațiile din algoritmul adunării în baza u se sistematizează astfel:

$$\begin{array}{l} a_m a_{m-1} \ldots a_1 a_0 + \\ \underline{b_m b_{m-1} \ldots b_1 b_0} \\ c_{m+1} c_m c_{m-1} \ldots c_1 c_0 \\ \\ \varepsilon_m \varepsilon_{m-1} \ldots \varepsilon_1 \varepsilon_0 \end{array}$$

ultima linie, care descrie transportul unității, de regulă se omite.

Astfel, dacă $u = 2$, $a = 1011101_{(2)}$, $b = 101101_{(2)}$, atunci $a + b$ se face după cum urmează:

$$\begin{array}{r} 1\,0\,1\,1\,1\,0\,1 + \\ \underline{\quad 1\,0\,1\,1\,0\,1} \\ 1\,0\,0\,0\,1\,0\,1\,0 \\ 1\,1\,1\,1\,1\,0\,1 \end{array}$$

deci $a + b = 10001010_{(2)}$. S-a folosit și tabla adunării numerelor naturale <2, care este

+	0	1
0	0	1
1	1	10

rezultatele fiind reprezentate în baza 2.

Se va arăta în continuare că înmulțirea a două numere naturale în baza u se reduce la următoarele tipuri de operații:

1° înmulțirea unui număr natural a cu o putere u^j a bazei u;

2° înmulțirea unui număr natural a cu o cifră a sistemului de numerație (deci cu un număr natural j, $0 \leqslant j < u$):

3° adunarea în baza u.

Fie

$$a = a_m a_{m-1} \ldots a_1 a_{0(u)} = a_m u^m + a_{m-1} u^{m-1} + \ldots$$
$$\ldots + a_1 u + a_0.$$

Atunci

$$au^j = a_m u^{m+j} + a_{m-1} u^{m-1+j} + \ldots + a_1 u^{1+j} + a_0 u^j =$$
$$= a_m a_{m+1} \ldots a_1 a_0 \underbrace{00 \ldots 0}_{j}{}_{(u)}$$

și acum este clar cum se face în baza u o înmulțire de tipul 1°.

Dacă i și j sînt două numere naturale $< u$, atunci $ij < u^2$, de unde, folosind teorema împărțirii cu rest pentru numere naturale, avem

$$ij = uq(i, j) + r(i, j), \quad 0 \leqslant r(i, j) < u, \quad 0 \leqslant q(i, j) < u, \tag{3.5}$$

cîtul $q = q(i, j)$ și restul $r = r(i, j)$ împărțirii numărului ij prin u depinzînd de i și j.

Fie acum a un număr natural dat în bază u:

$$a = a_m a_{m-1} \dots a_1 a_{0(u)} = \sum_{i=0}^{m} a_i u^i$$

și j o cifră a sistemului de numerație de bază u, deci $0 \leqslant j < u$. Avem

$$aj = \sum_{i=0}^{m} a_i j u^i = \sum_{i=0}^{m} (uq(a_i, j) + r(a_i, j))u^i =$$

$$= \sum_{i \geqslant 0} r(a_i, j)u^i + \sum_{i \geqslant 0} q(a_i, j)u^{i+1},$$

deci efectuarea produsului aj în baza u revine la a face suma în baza u a numerelor a', a'' reprezentate în baza u:

$$a' = r(a_0, j) + r(a_1, j)u + r(a_2, j)u^2 + \dots$$

și

$$a'' = q(a_0, j)u + q(a_1, j)a^2 + \dots$$

Așadar, s-a lămurit cum se face în baza u și o înmulțire de tipul 2°.

În sfîrșit, dacă $b = b_n b_{n-1} \dots b_1 b_0 = \sum_{j=0}^{n} b_j u^j$, atunci $ab = \sum_{j=0}^{n} ab_j u^j$, deci produsul ab se poate efectua făcînd suma în baza u a numerelor $ab_j u^j$, $j = 0, 1, 2, \dots, n$. Dar $ab_j u^j = (ab_j)u^j$. Așadar ab_j este o operație de tipul 2° și în sfîrșit $(ab_j)u^j$ o operație de tipul 1°.

Cititorul se poate convinge ușor că regula de înmulțire a numerelor naturale în baza zece se motivează din punct de vedere teoretic prin considerațiile de mai sus, luînd $u = 10$. Un instrument important al înmulțirii numerelor în baza zece este tabla înmulțirii numerelor < 10. Pe de altă parte, se observă că în regula de înmulțire a numerelor în baza u trebuie să cunoaștem numerele

$$q(i, j) \text{ și } r(i, j),\ 0 \leqslant i, j < u,$$

din relația (3.5). Din (3.5) rezultă că $q(i, j)$ și $r(i, j)$ sînt cifrele numărului ij, $0 \leqslant i, j < u$, reprezentat în baza u [dacă $ij < u$, avem $q(i, j) = 0$]. Așadar, procedeul de înmulțire expus uzează de tabla înmulțirii numerelor naturale $< u$, cu rezultatele reprezentate în baza u.

În tabelele 4 și 5 sînt date tablele înmulțirii în baza $u = 5$, respectiv $u = 2$.

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

Tabelul 4. Tabla înmulțirii în baza 5

×	0	0
0	0	0
1	0	11

Tabelul 5. Tabla înmulțirii în baza 2.

Încheiem acest paragraf cu cîteva considerații asupra algoritmului sistemelor de numerație. Fiind dat un număr natural $a > 0$, reprezentarea acestuia într-o bază u se poate face pe o idee de calcul dată de lema 6.1. Conform acesteia, cifra de rang 0 a lui a în baza u, anume a_0, este restul împărțirii lui a prin u. Dacă $q_0 = \left[\frac{a}{u}\right]$, atunci cifra de rang 1 a lui a în baza u, anume a_1, este restul împărțirii lui q_0 prin u. Dacă $q_1 = \left[\frac{q_0}{u}\right]$, atunci cifra de rang 2 a lui a în baza u, anume a_2, este restul împărțirii lui q_1 prin u, ș.a.m.d. După un număr finit de pași se obține $q_n = 0$ și atunci $a_n = q_{n-1}$ este cifra lui a de rang cel mai mare diferită de zero și avem

$$a = a_n a_{n-1} \ldots a_{0(u)}.$$

Scanned with OKEN Scanner

Introducînd două variabile q şi n, putem da următorul algoritm de reprezentare a numerelor naturale într-o bază u, numit algoritmul sistemelor de numeraţie.

N_1. $q \leftarrow a$, $n \leftarrow 0$.

N_2. $a_n \leftarrow q \bmod u$.

N_3. $q \leftarrow \left[\frac{q}{u}\right]$.

N_4. Dacă $q = 0$, treci la instrucţiunea N_6.

N_5. $n \leftarrow n + 1$ şi treci la instrucţiunea N_2.

N_6. STOP.

Schema logică a algoritmului sistemelor de numeraţie este dată în fig. 9.

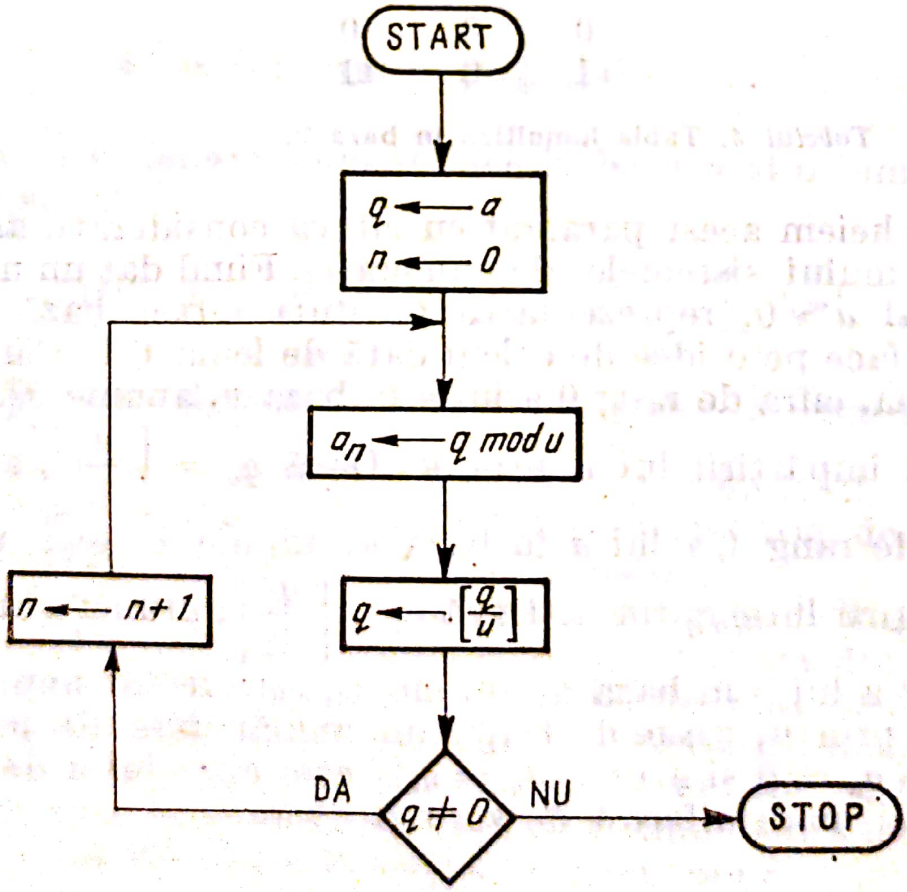


Fig. 9. Schema logică a algoritmului sistemelor de numeraţie.

Pentru calculul cu „creionul și hîrtia" calculele pot fi sistematizate ca în fig. 10.

Trebuie observat că numărul natural a ce urmează să fie reprezentat într-o bază u este dat, de regulă, într-o bază v și de fapt se face trecerea lui a din baza v în baza u. Se pot distinge trei variante :

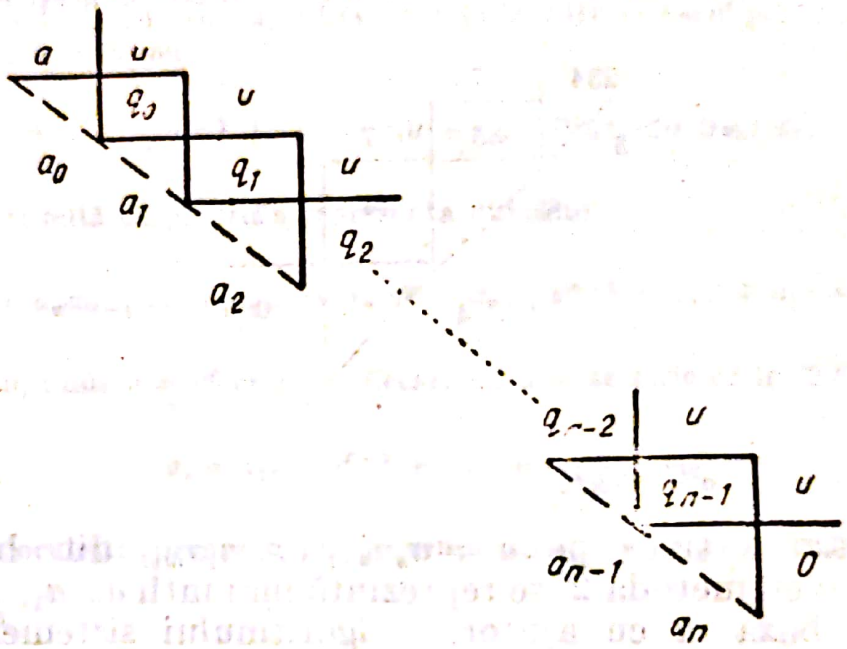


Fig. 10.

1° Trecerea lui a din baza v în baza u cu efectuarea calculelor în baza v.

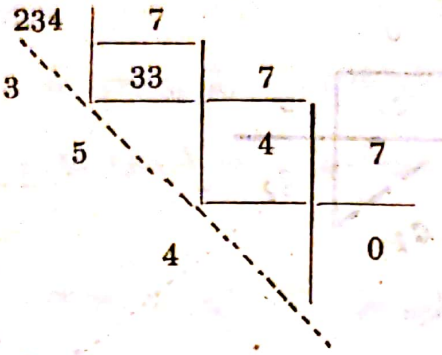
2° Trecerea lui a din baza v în baza u cu efectuarea calculelor în baza u.

3° Trecerea lui a din baza v în baza u cu efectuarea calculelor într-o bază intermediară w.

Pentru a trece pe a din baza v în baza u cu metoda 1° se reprezintă mai întîi u în baza v și apoi se aplică algoritmul sistemelor de numerație pentru a și u cu efectuarea calculelor în baza v. Cum în calculatoare numerele sînt, de regulă, reprezentate în baza $v = 2$, metoda 1° se aplică atunci cînd se livrează rezultatele numerice (de regulă în baza $u = 10$), execuția algoritmului sistemelor de numerație putînd fi astfel încredințată calculatoru-

lui (calculele se fac în baza $v = 2$). Aceeaşi metodă se aplică şi cînd se trece cu „hîrtia şi creionul" un număr din baza $v = 10$, într-o altă bază u, preferîndu-se calculele în baza $v = 10$ din motive lesne de înţeles.

Pentru exemplificare, să trecem numărul $a = 234$ dat în baza $v = 10$ în baza $u = 7$. Folosind dispunerea calculelor propusă în fig. 8, algoritmul sistemelor de numeraţie (perfectat în baza $v = 10$) este în acest caz



de unde

$$a = 453_{(7)}.$$

Pentru a trece pe $a = a_n a_{n-1} \ldots a_1 a_{0(v)}$ din baza v în baza u cu metoda 2° se reprezintă mai întîi $a_0, a_1, \ldots, a_n$ şi v în baza u cu ajutorul algoritmului sistemelor de numeraţie. Se introduc $a_0, a_1, \ldots, a_n$ şi v astfel reprezentaţi în expresia

$$a_n v^n + a_{n-1} v^{n-1} + \ldots + a_1 v + a_0$$

şi se face calculul acesteia folosind algoritmul adunării şi algoritmul înmulţirii în baza u. Se obţine, în final, reprezentarea lui a în baza u. Această metodă este folosită la introducerea datelor numerice în calculator. Numerele date de regulă în baza $v = 10$ se reprezintă în calculator în baza $u = 2$; efectuarea calculelelor în baza $u = 2$ poate fi încredinţată calculatorului.

Metoda 3° este evident o combinaţie a primelor două. Astfel, dacă dorim să trecem un număr a dintr-o bază $v \neq 2$, într-o bază $u \neq 2$, folosind un calculator care lucrează cu numere reprezentate în baza 2, atunci trecem pe a în baza 2 cu metoda 2° şi apoi îl trecem în baza u cu metoda 1°. Procedînd astfel, toate calculele pot fi încredinţate calculatorului. Cînd $v \neq 10$ şi $u \neq 10$, iar

trecerea de la baza b la baza u vrem să o facem cu „creionul și hîrtia", preferăm baza intermediară $w = 10$ pentru a putea executa toate calculele în baza 10, cu care sîntem obișnuiți.

Observații. 1. Trecerea unui număr natural a din baza v în baza u se simplifică considerabil cînd $v = u^r$, cu r număr natural $\geqslant 1$. Metoda se justifică prin faptul că un număr natural $b < n^r$ poate fi scris în mod unic sub forma

$$b = c_{r-1}u^{r-1} + \ldots + c_1 u + c_0, \quad 0 \leqslant c_i < u, 0 \leqslant i < r. \tag{3.6}$$

De aici, rezultă că pentru a reprezenta numărul

$$a = a_n a_{n-1} \ldots a_1 a_{0(v)} = a_n v^n + a_{n-1} v^{n-1} + \ldots + a_1 v + a_0$$

în baza u, unde $v = u^r$ cu $r > 1$, fiecare cifră a_i se scrie ca în (3.6), anume

$$a_i = c_{ir-1} u^{r-1} + \ldots + c_{i1} u + c_{i0}$$

și se înlocuiește fiecare a_i cu secvența $c_{ir-1} \ldots c_{i1} c_{i0}$, deci obținem secvența

$$c_{nr-1} \ldots c_{n1} c_{n0} c_{n-1,r-1} \ldots c_{n-11} c_{n-10} \ldots c_{01} c_{00}. \tag{3.7}$$

Înlăturînd cifrele egale cu 0 de la începutul secvenței (3.7) se obține reprezentarea lui a în baza u.

Astfel, pentru a reprezenta numărul $a = 375_{(8)}$ în baza $u = 2$ (deci $v = u^3$), scriem mai întîi

$$a_0 = 4 = 1 \times 2^2 + 0 \times 2 + 1 \times 1 = c_{02} \cdot 2^2 + c_{01} \cdot 2 + c_{00}$$
$$a_1 = 7 = 1 \times 2^2 + 1 \times 2 + 1 \times 1 = c_{12} \cdot 2^2 + c_{11} \cdot 2 + c_{10},$$
$$a_2 = 3 = 0 \times 2^2 + 1 \times 2 + 1 \times 1 = c_{22} \cdot 2^2 + c_{21}, \cdot 2^2 + c_{20},$$

așadar (3.7) este în acest caz secvența

$$0\,1\,1 \quad 1\,1\,1 \quad 1\,0\,1.$$

2. Cînd $v^r = u$, $r \geqslant 1$, trecerea unui număr din baza v în baza u se face printr-o metodă care urmează calea inversă a metodei de la observația 1. În acest caz, pentru a trece în baza u numărul $a = a_n a_{n-1} \ldots a_{0(v)}$ se separă de la dreapta la stînga grupe de cîte r cifre (ultima grupă avînd cel mult r cifre) și fiecare grupă va reprezenta o cifră în baza u, cu care vom

înlocui grupa respectivă. Se obține astfel reprezentarea lui a în baza u. Astfel, dacă $u = 8$ și $v = 2$, deci $v^3 = u$, numărul

$$a = 11\,111\,101_{(2)}$$

are în baza 8 reprezentarea

$$a = 375_{(8)}$$

pentru că cifrele lui a din baza 2 pot fi grupate astfel:

$$\underbrace{11}\ \underbrace{111}\ \underbrace{101}$$

și grupele obținute reprezintă în baza 2 respectiv cifrele 3, 7 și 5 ale bazei 8.

3. Inconvenientul sistemului binar de numerație constă în faptul că reprezentarea numerelor mari necesită secvențe de cifre binare exagerat de lungi. Aceasta complică mult lectura numerelor precum și aprecierea ordinului lor de mărime. O metodă de a atenua aceste inconveniente este de a folosi sisteme de numerație cu baze mixte. Un exemplu este sistemul de numerație zecimal codat în binar. În acest sistem de numerație numerele se reprezintă în zecimal iar cifrele sale în binar, rezervîndu-se cîte patru poziții binare fiecărei cifre zecimale. Astfel, numărul $a = 793_{(10)}$ se reprezintă în sistemul zecimal codat în binar după cum urmează:

$$\underbrace{0111}_{7}\ \underbrace{1001}_{9}\ \underbrace{0011}_{3}$$

În practică se folosește curent sistemul de numerație cu baza mixtă. Astfel expresia

8 ani, 3 luni, 2 săptămîni, 3 zile, 15 ore și 35 minute

este un model de reprezentare a timpului într-un sistem de numerație cu șase baze.

§ 7. Algoritmul binar

Așa cum am menționat în paragraful precedent, calculatoarele electronice utilizează de regulă reprezentarea numerelor naturale în baza 2. Se observă că într-o asemenea reprezentare ultima cifră binară (cifra de rang 0) a unui număr par este egală cu 0. Rezultă imediat că dacă a este par, atunci reprezentarea binară a lui $a/2$ se obține din aceea a lui a înlăturînd cifra de rang 0. O situație asemănătoare o întîlnim la împărțire prin 10 a multiplilor lui 10 dați în baza 10. Așadar, împărțirea cu 2 în calculatoare electronice ce lucrează cu numere în baza 2 este o operație extrem de simplă. Algoritmul

binar are la bază ideea de a exploata această împrejurare pentru calculul celui mai mare divizor comun a două numere întregi.

Dacă $a,\ b \in \mathbb{Z}$, atunci

$$(a,\ b) = (-a,\ b) = (a,\ -b) = (-a,\ -b),$$

de unde rezultă că ne putem mărgini la cazul cînd $a > 0$ și $b > 0$. Următorul rezultat ne va oferi argumentația pentru algoritmul binar.

Teorema 7.1. *Fie a și b două numere întregi pozitive.*

1) *Dacă a și b sînt pare, atunci* $(a,\ b) = 2(a/2,\ b/2)$.

2) *Dacă a este par și b impar, atunci* $(a,\ b) = (a/2,\ b)$.

3) *Dacă a este impar și b par, atunci* $(a,\ b) = (a,\ b/2)$.

4) *Dacă a și b sînt impari, atunci $a-b$ este par,*

$$|a - b| < \max\{a,\ b\}$$

și avem :

$$(a,\ b) = (a - b,\ b) = (a,\ b - a).$$

5) $(a,\ a) = a$.

Demonstrație. 1) Fie $a',\ b' \in \mathbb{N}$ astfel încît $a = 2a'$ și $b = 2b'$. Rezultă

$$(a,\ b) = (2a',\ 2b') = 2(a',\ b') = 2\left(\frac{a}{2},\ \frac{b}{2}\right).$$

2) Este suficient de arătat că

$$D\langle a,\ b\rangle = D\langle a',\ b\rangle,$$

unde $a' \in \mathbb{N}$, astfel încît $2a' = a$. Este clar că din $c \in D\langle a',\ b\rangle$ rezultă $c \in D\langle a,\ b\rangle$. Reciproc, fie $c \in D\langle a,\ b\rangle$. Cum $c \mid b$ și b este impar, rezultă că c este impar. Așadar,

2 nu devide pe c, de unde $(c, 2) = 1$. Dar $(c, 2) = 1$ și $c \mid 2a'$ implică $c \mid a'$ (vezi corolarul 3.3), de unde $c \in D\langle a', b\rangle$.

3) Se demonstrează la fel ca 2).

4) Este clar că dacă a și b sînt impare, atunci $a - b$ este par. De asemenea, dacă a și b sînt > 0, atunci, evident, $|a - b| < \max\{a, b\}$. Cum

$$a = b \times 1 + (a - b) \text{ și } b = a \times 1 + b - a,$$

ultima afirmație de la 4) rezultă din lema 4.1.

5) Este evident.

Să încercăm să folosim rezultatele din teorema 7.1 pentru a calcula (a, b). Fie e cel mai mare număr întreg $\geqslant 0$ astfel încît

$$2^e \mid a \text{ și } 2^e \mid b.$$

Fie $a', b' \in \mathbb{N}$ astfel încît $a = 2^e a'$ și $b = 2^e b'$. Din modul în care a fost ales e rezultă că cel puțin unul din numerele a' și b' este impar. Avem

$$(a, b) = 2^e (a', b')$$

și la aceasta se ajunge aplicînd 1) din teorema 7.1 de e ori.

Dacă $a' = b'$, atunci este situația 5) din teorema precedentă, deci

$$(a', b') = a' = b',$$

de unde

$$(a, b) = 2^e a'.$$

Dacă $a' \neq b'$, a' fiind par și b' impar, atunci folosind 2) de un număr finit de ori, se ajunge la situația

$$(a', b') = (a'', b'), \ a'' < a',$$

cu a'' și b' impari.

Dacă $a' \neq b'$, a' impar şi b' par, atunci folosind 3) de un număr finit de ori, se obţine

$$(a', b') = (a', b''), b' < 'b',$$

cu a' şi b'' impari.

Fie a' şi b' impari şi $a' > b'$. Atunci $a' - b'$ este un număr par strict pozitiv şi conform cu 4) rezultă

$$a', b') = (a' - b', b'), \quad 0 < a' - b' < a' = \max\{a', b'\},$$

deci se dă peste situaţia din 2).

La fel, dacă a' şi b' sînt impari, $a' < b'$, atunci se obţine 3) prin

$$(a', b') = (a', b' - a),$$

unde $0 < b' - a' < b' = \max\{a', b'\}$ etc.

Se observă că în fiecare etapă cel puţin unul din numerele a, b se micşorează cu cel puţin o unitate, rămînînd $\geqslant 0$. Dar cum la plecare avem la dispoziţie $a + b$ unităţi, după un număr finit de paşi se obţine situaţia 5), deci se oţine $a' = b'$ şi atunci $(a, b) = 2^e a'$.

Din analiza făcută este uşor să se conceapă un algoritm de calcul al celui mai mare divizor comun d pentru două numere naturale a şi b. Se introduc variabilele x, y, k pentru a putea redacta următorul algoritm, numit algoritmul binar.

B_1. $x \leftarrow a$, $y \leftarrow b$, $k \leftarrow 0$.

B_2. Dacă $2 \notin D\langle x, y\rangle$, treci la instrucţiunea B_4.

B_3. $x \leftarrow \frac{x}{2}$, $y \leftarrow \frac{y}{2}$, $k \leftarrow k + 1$ şi mergi la B_2.

B_4. Dacă 2 nu divide x, treci la instrucţiunea B_6.

B_5. $x \leftarrow \frac{x}{2}$ şi treci la B_4.

B_6. Dacă 2 nu divide y, treci la instrucţiunea B_{10}.

B_7. $y \leftarrow \frac{y}{2}$ și treci la B_6.

B_8. Dacă x nu este strict mai mare ca y, treci la B_{10}.

B_9. $x \leftarrow x - y$ și treci la B_5.

B_{10}. Dacă x nu este strict mai mic ca y, treci la B_{12}.

B_{11}. $y \leftarrow y - x$ și treci la B_7.

B_{12}. $d \leftarrow 2^k x$.

Schema logică a algoritmului binar este dată în fig. 11.

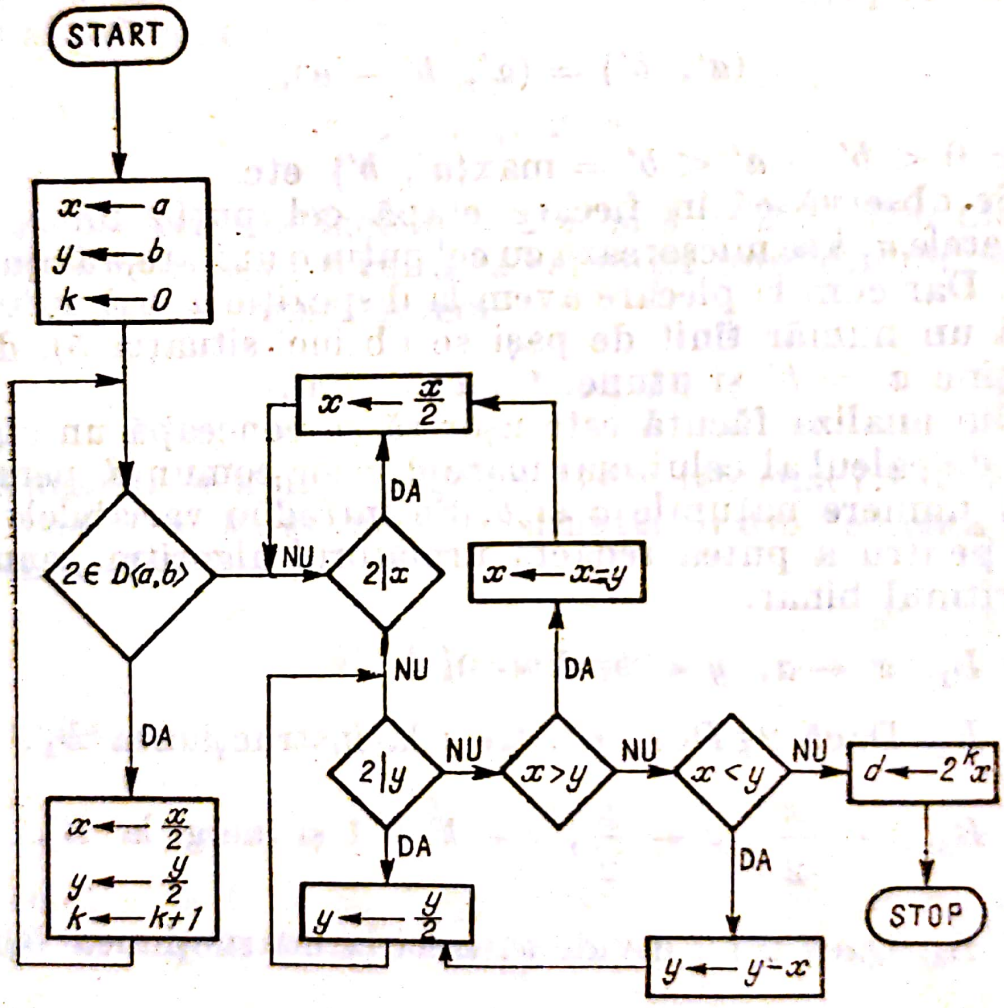


Fig. 11. Schema logică a algoritmului binar.

Să aplicăm algoritmul binar pentru calculul lui (840, 156). În tabelul 6 sînt date valorile pe care le iau variabilele x, y, k în acest caz.

Scanned with OKEN Scanner

x	y	k
840	156	0
420	78	1
210	39	2
105	39	2
66	39	2
33	39	2
33	6	2
33	3	2
30	3	2
15	3	2
12	3	2
6	3	2
3	3	2

Tabelul 6

Algoritmul binar se sfîrşeşte cînd valorile lui x şi y devin egale. În tabelul 6 se observă că acesta se realizează pe ultima linie. Avem

$$(840,\ 156) = 2^2(3,\ 3) = 4 \times 3 = 12.$$

Inele cu descompunere unică în factori primi

§ 1. Inele factoriale

Fie A un domeniu de integritate.

Definiția 1.1. Un element p nenul și neinversabil din A se numește *prim*, dacă oricare ar fi a și b din A din

$$p \mid ab \Rightarrow p \mid a \text{ sau } p \mid b.$$

Un element π nenul și neinversabil din A se numește *ireductibil* dacă din

$$a \mid \pi \Rightarrow a \sim 1 \text{ sau } a \sim \pi.$$

Un element nenul și neinversabil, care nu este ireductibil, se numește *reductibil*.

Cu alte cuvinte, elementele prime ale inelului A sînt elementele $p \neq 0$, neinversabile care divid un produs de elemente din A dacă și numai dacă divid cel puțin unul dintre factori, iar elementele ireductibile ale inelului A sînt elementele $\pi \neq 0$ neinversabile care, mai puțin o asociere în divizibilitate, admit ca divizori doar pe 1 și π.

Scanned with OKEN Scanner

Propoziţia 1.1. *Orice element prim este ireductibil.*

Demonstraţie. Fie p un element prim al inelului A şi $a \in A$ un divizor al lui p. Există $b \in A$ astfel încît $p = ab$. Relaţia $1 \cdot p = ab$ atrage că $p \mid ab$ şi cum p este prim, rezultă $p \mid a$ sau $p \mid b$. Dacă $p \mid a$, atunci $a = pc$ cu $c \in A$. Din $1 \cdot p = ab = pcb$ rezultă $1 = cb$, deci $b \in U_A$, de unde $a \sim p$. Dacă $p \mid b$, se deduce analog că $a \sim 1$. Aşadar, p este element ireductibil al lui A.

Observaţie. Reciproca afirmaţiei din propoziţia precedentă nu este adevărată, în general.

Iată un exemplu în acest sens. Fie A mulţimea tuturor numerelor complexe de forma

$$a + b\sqrt{5}\,\mathrm{i},\ a, b \in \mathbb{Z}.$$

Cum

$$(a + b\sqrt{5}\,\mathrm{i}) + (c + d\sqrt{5}\,\mathrm{i}) = (a + c) + (b + d)\sqrt{5}\,\mathrm{i}$$

şi

$$(a + b\sqrt{5}\,\mathrm{i})(c + d\sqrt{5}\,\mathrm{i}) = (ac - 5bd) + (ad + bc)\sqrt{5}\,\mathrm{i},$$

rezultă că suma, respectiv produsul a două numere complexe din A se găseşte în A. Deci A are structură de inel faţă de adunarea şi înmulţirea numerelor complexe.

Fie

$$N : A \to \mathbb{N},\ N(z) = \|z\| = z\bar{z} = a^2 + 5b^2,$$

oricare ar fi $z = a + b\sqrt{5}\,\mathrm{i} \in A$. Dar $N(z_1 z_2) = N(z_1)N(z_2)$, oricare ar fi z_1 şi z_2 din A (vezi § 1, cap. III). Dacă $a + b\sqrt{5}\,\mathrm{i} \in A$ este inversabil, există $c + d\sqrt{5}\,\mathrm{i} \in A$ astfel încît

$$(a + b\sqrt{5}\,\mathrm{i})(c + d\sqrt{5}\,\mathrm{i}) = 1.$$

Cum

$$1 = N(1) = N(a + b\sqrt{5}\,\mathrm{i})N(c + d\sqrt{5}\,\mathrm{i}) = (a^2 + 5b^2)(c^2 + 5d^2),$$

rezultă că $a^2 + 5b^2 = 1$, de unde $a = \pm 1$ şi $b = 0$. Deducem că $U_A = \{-1, 1\}$.

Evident, în inelul A are loc identitatea

$$3 \cdot 7 = (1 + 2\sqrt{5}\,\mathrm{i})(1 - 2\sqrt{5}\,\mathrm{i}).$$

Scanned with OKEN Scanner

Numărul 3 este element ireductibil al inelului A. Într-adevăr, dacă $z = a + b\sqrt{5}\,i$ divide 3, atunci $N(z) \mid N(3)$. Cum $N(z) = a^2 + 5b^2$ iar $N(3) = 9$, trebuie ca $a^2 + 5b^2 = 1$ sau $a^2 + 5b^2 = 3$ sau $a^2 + 5b^2 = 9$. Cum ecuația $a^2 + 5b^2 = 3$ nu are soluții întregi, iar ecuațiile $a^2 + 5b^2 = 1$ și $a^2 + 5b^2 = 9$ au doar soluțiile $a = \pm 1$, $b = 0$, respectiv $a = \pm 2$, $b = \pm 1$ și $a = \pm 3$, $b = 0$, se verifică imediat că singurii divizori ai lui 3 în A sînt ± 1 și ± 3, deci $z \sim 1$ sau $z \sim 3$ în A, de unde rezultă că 3 este element ireductibil al inelului A. Cum $N(1 + 2\sqrt{5}\,i) = N(1 - 2\sqrt{5}\,i) = 1 + 20 = 21$, iar $N(3) = 9$ nu divide 21, rezultă că 3 nu divide nici pe $1 + 2\sqrt{5}\,i$, nici pe $1 - 2\sqrt{5}\,i$, cu toate că divide produsul lor. Așadar, 3 nu este element prim al inelului A.

Într-o clasă largă de inele elementele ireductibile coincid cu cele prime. Se va arăta, mai întîi, că acest lucru este adevărat pentru inelele euclidiene. Așadar, în particular în inelele $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ elementele ireductibile coincid cu cele prime. Tot în acest paragraf sînt descrise inelele în care orice element nenul și neinversabil se reprezintă în mod unic (mai puțin o asociere în divizibilitate) ca produs de elemente ireductibile (prime), numite inele factoriale. Se va arăta că inelele euclidiene sînt inele factoriale. Pentru asemenea inele este important să descriem elementele ireductibile.

Să observăm că dacă un element p (respectiv π) într-un domeniu de integritate A este prim (ireductibil), atunci pentru orice $u \in U_A$ elementul up (respectiv $u\pi$) este prim (ireductibil). De asemenea, dacă (A, φ) este un inel euclidian și $a \in A$, atunci

$$\varphi(a) > 1 \Leftrightarrow a \neq 0 \text{ și } a \notin U_A$$

și

a reductibil $\Leftrightarrow$ există $b, c \in A$, astfel încît

$$a = bc, \quad 1 < \varphi(b) < \varphi(a), \quad 1 < \varphi(c) < \varphi(a).$$

Propoziția 1.2. *Într-un inel euclidian (A, φ) orice element $a \in A$ cu $\varphi(a) > 1$ admite cel puțin un divizor ireductibil.*

Demonstrație. Mulțimea de numere naturale

$$P = \{\varphi(d) \mid d \mid a,\ \varphi(d) > 1\}$$

Scanned with OKEN Scanner

nu este vidă, întrucît conține pe $\varphi(a)$. Fie $\pi \in A$, astfel încît $\varphi(\pi)$ este primul element al lui P. Dacă π este reductibil, atunci există b, $c \in A$, astfel încît

$$\pi = bc,\ 1 < \varphi(b) < \varphi(\pi),\ 1 < \varphi(c) < \varphi(\pi).$$

Rezultă că $\varphi(b)$ și $\varphi(c)$ sînt din P, ceea ce contrazice alegerea lui π. Rămîne adevărat că π este ireductibil și teorema este demonstrată.

Teorema 1.3. *Într-un inel euclidian* (A, φ) *orice element* $a \neq 0$ *neinversabil este produsul unui număr finit de elemente ireductibile.*

Demonstrație. Dacă a este ireductibil, nu mai este nimic de demonstrat. Dacă a este reductibil, atunci există b, $c \in A$ astfel încît

$$a = bc,\ 1 < \varphi(b) < \varphi(a),\ 1 < \varphi(c) < \varphi(a).$$

Presupunînd că teorema este adevărată pentru elemente $x \in A$ cu $1 < \varphi(x) < \varphi(a)$, rezultă că b și c sînt produse finite de elemente ireductibile și atunci $a = bc$ are aceeași proprietate.

Propoziția 1.4. *Într-un inel euclidian* (A, φ) *orice element ireductibil este prim.*

Demonstrație. Presupunem prin absurd că există elemente ireductibile care nu sînt prime. Fie printre acestea elementul ireductibil π astfel încît $\varphi(\pi)$ este minim. Cum π nu este prim, există a, $b \in A$, astfel încît $\pi \mid ab$ și π nu divide nici pe a, și nici pe b. Avem $\varphi(a) > 1$ și $\varphi(b) > 1$. Într-adevăr, dacă $\varphi(a) = 0$, atunci $a = 0$ și deci $\pi \mid a$. Dacă $\varphi(a) = 1$, atunci $a \in U_A$ și din $\pi \mid ab$ rezultă $\pi \mid b$. Așadar, $\varphi(a) > 1$ și la fel se arată că $\varphi(b) > 1$. Se poate presupune că $\varphi(a) < \varphi(\pi)$ și $\varphi(b) < \varphi(\pi)$. Într-adevăr, putem scrie $a = \pi q + r$ cu $\varphi(r) < \varphi(\pi)$ și din egalitatea

$$ab = \pi qb + rb$$

rezultă că $\pi \mid rb$, π nu divide r și π nu divide b. Deci putem înlocui pe a cu r cînd $\varphi(a) \geqslant \varphi(\pi)$. Analog se procedează

Scanned with OKEN Scanner

cînd $\varphi(b) \geqslant \varphi(\pi)$. Putem presupune chiar că a și b sînt astfel încît $\varphi(a)\varphi(b)$ este minim. Fie $c \in A$ astfel încît $ab = ac$. Rezultă $\varphi(c) > 1$, deoarece altfel $a \sim \pi$ sau $b \sim \pi$. Cum $\varphi(c) > 1$, elementul c admite un divizor ireductibil (vezi propoziția 1.2), fie acesta π_1. Din

$$\varphi(\pi)\varphi(c) = \varphi(a)\varphi(b) < \varphi(\pi)\varphi(\pi)$$

rezultă că $\varphi(c) < \varphi(\pi)$. Cum $\varphi(\pi_1) \leqslant \varphi(c) < \varphi(\pi)$, $\pi_1 \mid ab$ și din modul cum a fost ales π, rezultă că $\pi_1 \mid a$ sau $\pi_1 \mid b$. Presupunem că $\pi_1 \mid a$ și fie a_1, $c_1 \in A$ astfel încît $c = c_1\pi_1$ și $a = a_1\pi_1$. Din $a_1\pi_1 b = \pi c_1 \pi_1$ rezultă $a_1 b = \pi c_1$. Așadar, $\pi \mid a_1 b$ și evident π nu divide nici pe a_1 și nici pe b. Cum $\varphi(a_1)\,\varphi(b) < \varphi(a)\varphi(b)$, este contrazisă alegerea lui a și b.

Teorema 1.5. *Fie* (A, φ) *un inel euclidian și* $a \in A$ *astfel încît* $\varphi(a) > 1$. *Dacă*

$$a = \pi_1\pi_2 \ldots \pi_m = \pi_1'\pi_2' \ldots \pi_n',$$

unde π_i *și* π_j' *sînt elemente ireductibile ale lui* A, *atunci* $m = n$ *și*

$$\pi_i \sim \pi'_{\sigma(i)} \qquad i = 1, 2, \ldots, n,$$

unde σ *este o permutare a numerelor* $1, 2, \ldots, n$.

Demonstrație. Din egalitatea din enunț rezultă că π_1 divide produsul $\pi_1'\pi_2' \ldots \pi_n'$. Cum π_1 este element prim al lui A din propoziția precedentă, rezultă că există j, $1 \leqslant j \leqslant n$, astfel încît $\pi_1 \mid \pi_j'$. Schimbînd eventual indexarea elementelor π_j', putem presupune că $j = 1$. Deoarece π_1' este ireductibil iar π_1 este nenul și neinversabil, rezultă că $\pi_1 \sim \pi_1'$, deci $\pi_1' = \pi_1 u$ cu $u \in U_A$. Avem

$$b = \pi_2\pi_3 \ldots \pi_m = (u\pi_2')\pi_3' \ldots \pi_n', \tag{4.1}$$

unde $u\pi_2'$ este ireductibil (deoarece $u \in U_A$ și π_2' este ireductibil) iar b este cîtul împărțirii lui a prin π_1. Din definiția elementelor ireductibile rezultă că afirmația din enunț

Scanned with OKEN Scanner

este adevărată cînd a este element ireductibil al lui A. Presupunînd teorema adevărată pentru elemente $b \in A$ care admit o descompunere într-un produs de $m-1$ elemente ireductibile, din (4.1) rezultă că $m-1=n-1$, deci $m=n$ și, mai puțin o permutare,

$$\pi_i \sim \pi_i', \quad i = 2, 3, \ldots, m.$$

Cum și $\pi_1 \sim \pi_1'$, teorema este astfel demonstrată prin inducție.

Definiția 1.2. Un domeniu de integritate A în care orice element nenul și neinversabil se reprezintă în mod unic, mai puțin o asociere în divizibilitate, ca produs de elemente prime se numește *inel factorial.*

Corolarul 1.6. *Orice inel euclidian este factorial.*

Cum inelele $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ sînt euclidiene, rezultă că în aceste inele elementele ireductibile coincid cu elementele prime. Mai mult, aceste inele sînt factoriale sau, cu o altă terminologie, inele cu descompunere unică în factori primi. În paragraful următor se va arăta că inelul $\mathbb{Z}[X]$ este factorial.

Pripoziția 1.7. *Într-un inel factorial A orice element ireductibil este prim.*

Demonstrație. Fie π un element ireductibil al inelului A. Cum A este factorial, există în A elementele prime $p_1, \ldots, p_n$ astfel încît $\pi = p_1 p_2 \ldots p_n$. Dacă $n > 1$, atunci p_1 este un divizor al lui π astfel încît $p_1 \sim 1$ și $p_1 \sim \pi$, ceea ce nu este posibil, deoarece π este ireductibil. Rezultă că $n = 1$ și atunci $\pi = p_1$, deci π este prim.

Majoritatea problemelor care se pun pentru inele factoriale se tratează folosind descompunerea elementelor acestor inele în produs de elemente prime (ireductibile). Așadar, fiind dat un inel factorial A este important de rezolvat următoarele două probleme:

I) Descrierea elementelor prime (ireductibile) ale inelului A.

D) Găsirea unor procedee eficiente de descompunere în factori ireductibili (primi) a elementelor lui A și, legat

Scanned with OKEN Scanner

de aceasta, găsirea divizorilor primi (ireductibili) ai unui element dat din A.

Ne vom ocupa în continuare de aceste probleme. În § 2 se va arăta că problema I) are o rezolvare completă pentru inelele $\mathbb{R}[X]$ și $\mathbb{C}[X]$ și parțială pentru inelele $\mathbb{Z}[X]$ și $\mathbb{Q}[X]$. În § 3 se vor da cîteva rezultate în legătură cu probleme I) și D) în inelul $\mathbb{Z}$.

§ 2. Elemente ireductibile în inele de polinoame

Fie A un domeniu de integritate și $A[X]$ inelul polinoamelor în nedeterminata X cu coeficienți în A. Fie f și g două polinoame nenule din $A[X]$:

$$f = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0,\ a_i \in A,\ a_m \neq 0,$$

$$g = b_n X^n + b_{n-1} X^{n-1} + \ldots + b_1 X + b_0,\quad b_j \in A,\ b_n \neq 0.$$

Atunci

$$fg = a_m b_n X^{m+n} + (a_m b_{n-1} + a_{m-1} b_n) X^{m+n-1} + \ldots$$

$$\ldots + (a_1 b_0 + a_0 b_1) X + a_0 b_0$$

și cum $a_n b_m \neq 0$ (A fiind domeniu de integritate), rezultă că $fg \neq 0$, deci $A[X]$ este domeniu de integritate. Astfel, s-a demonstrat :

Propoziția 2.1. *Dacă A este un domeniu de integritate, atunci inelul de polinoame $A[X]$ este domeniu de integritate.*

Să observăm că dacă A este domeniu de integritate, $U_{A[X]} = U_A$. Cînd $A = K$ (corp), atunci polinoamele nenule și neinversabile din $K[X]$ sînt exact polinoamele de grad $\geqslant 1$.

Definiția 2.1. Fie A un domeniu de integritate și f un polinom nenul și neinversabil din $A[X]$. Se spune că f este *ireductibil peste A* dacă f este element ireductibil al inelului $A[X]$. În caz contrar, se spune că f este *reductibil peste A.*

Scanned with OKEN Scanner

Observații. 1. Fie K un corp. Atunci orice polinom ireductibil f peste K este asociat în divizibilitate cu un polinom unitar, ireductibil peste K (*polinom unitar* înseamnă un polinom cu coeficientul termenului de grad maxim în X egal cu 1).

Într-adevăr, dacă

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_n X + a_0, \qquad a_n \neq 0,$$

atunci

$$a_n^{-1} f = X^n + a_n^{-1} a_{n-1} X^{n-1} + \ldots + a_n^{-1} a_1 X + a_n^{-1} a_0$$

este unitar și ireductibil (deoarece $a_n^{-1} \in U_{K[X]}$ și deci $a_n^{-1} f$ este asociat în divizibilitate în inelul $K[X]$ cu polinomul ireductibil f). Este deci suficient să determinăm polinoamele unitare, ireductibile peste K.

2. Un polinom f nenul și neinversabil din $K[X]$ este ireductibil peste K dacă și numai dacă f nu poate fi reprezentat ca produs de două polinoame din $K[X]$, ambele cu gradul strict mai mic decît gradul lui f. În particular, rezultă că toate polinoamele de grad egal cu 1, cu coeficienți din K sînt ireductibile peste K.

Teorema 2.2. *Polinoamele de grad egal cu* 1 *cu coeficienți complecși sînt singurele polinoame ireductibile peste* $\mathbb{C}$.

Demonstrație. Din observația 2 rezultă că polinoamele de grad 1 din $\mathbb{C}[X]$ sînt elemente ireductibile ale acestui inel, deci polinoame ireductibile peste $\mathbb{C}$. Fie $g \in \mathbb{C}[X]$ astfel încît $n = \deg(g) > 1$. Cum orice polinom cu coeficienți complexi de grad >0 admite cel puțin o rădăcină complexă (teorema fundamentală a algebrei), există $z \in \mathbb{C}$ astfel încît $g(z) = 0$. Rezultă că $X - z$ devine $g(X)$ în inelul $\mathbb{C}[X]$. Așadar, există $h \in \mathbb{C}[X]$ astfel încît

$$g = (X - z)h.$$

Cum $\deg(X - z) = 1 < \deg g$ și $\deg(h) = n - 1 < \deg(g)$, rezultă că g este reductibil peste $\mathbb{C}$ și teorema este demonstrată.

Întrucît $\mathbb{C}[X]$ este inel factorial (vezi corolarul 1.6) și orice polinom ireductibil peste $\mathbb{C}$ este asociat în divizibilitate cu un polinom de forma $X - z$, cu $z \in \mathbb{C}$, rezultă :

Corolarul 2.3. *Orice polinom* $g \in \mathbb{C}[X]$ *de grad* >0 *se reprezintă în mod unic sub forma*

$$g = z(X - z_1)^{e_1} (X - z_2)^{e_1} \ldots (X - z_r)^{e_r},$$

Scanned with OKEN Scanner

unde $z, z_1, \ldots, z_r \in \mathbb{C}$, $z_i \neq z_j$ *pentru* $i \neq j$ *şi* $e_i \in \mathbb{N}$, $e_i \geq 1$, $i = 1, 2, \ldots, r$.

Teorema 2.4. *Polinoamele* $X - \alpha$ *şi* $X^2 - \beta X - \gamma$ *cu* $\alpha, \beta, \gamma \in \mathbb{R}$, $\beta^2 + 4\gamma < 0$ *sînt, mai puţin o asociere în divizibilitate, singurele polinoame ireductibile peste* $\mathbb{R}$.

Demonstraţie. Polinoamele $X - \alpha$, $\alpha \in \mathbb{R}$, fiind de gradul întîi, sînt ireductibile peste $\mathbb{R}$. Fie $g \in \mathbb{R}[X]$ un polinom de grad >1. Dacă g admite o rădăcină reală α, atunci $X - \alpha$ divide pe f în inelul $\mathbb{R}[X]$, deci există $h \in \mathbb{R}[X]$ astfel încît

$$g = (X - \alpha)h.$$

Cum gradele polinoamelor $X - \alpha$ şi h sînt strict mai mici ca gradul lui g, rezultă că g este reductibil peste $\mathbb{R}$.

Fie $f \in \mathbb{R}[X]$ un polinom ireductibil peste $\mathbb{R}$ de grad $n > 1$. Din cele de mai sus rezultă că f nu admite rădăcini reale. Fie $z \in \mathbb{C}$, $z = \rho + \delta i$, cu $\rho, \delta \in \mathbb{R}$, $\delta \neq 0$, o rădăcină complexă a lui f. Deoarece f are coeficienţii reali, din $f(z) = 0$ rezultă $f(\bar{z}) = 0$. Din $f(z) = 0$, rezultă că $X - z$ divide f în inelul $\mathbb{C}[X]$, deci există $g \in \mathbb{C}[X]$ astfel încît

$$f = (X - z)g.$$

Cum $z \neq (\delta \neq 0)$ şi

$$0 = f(\bar{z}) = (z - \bar{z})g(\bar{z}),$$

rezultă că $g(\bar{z}) = 0$, deci $g = (X - \bar{z})h$ cu $h \in \mathbb{C}[X]$, de unde

$$f = (X - z)(X - \bar{z})h = (X^2 - \beta X - \gamma)h$$

cu $\beta = 2\rho$ şi $\gamma = -\rho^2 - \delta^2$. Avem $\beta^2 + 4\gamma = -4\delta^2 < 0$. Cum f şi $X^2 - \beta X - \gamma$ au coeficienţii reali, algoritmul uzual al împărţirii lui f prin $X^2 - \beta X - \gamma$ arată că h are tot coeficienţi reali. Din $f = (X^2 - \beta X - \gamma)h$ şi ipoteza că f este ireductibil peste $\mathbb{R}$, rezultă că $\deg(h) = 0$, deci $n = 2$. Aşadar, un polinom f ireductibil peste $\mathbb{R}$ de grad > 1 este de forma $X^2 - \beta X - \gamma$ cu $\beta, \gamma \in \mathbb{R}$,

Scanned with OKEN Scanner

$\beta^2 + 4\gamma < 0$. Reciproc, un polinom $X^2 - \beta X - \gamma$ cu $\beta, \gamma \in \mathbb{R}$, $\beta^2 + 4\gamma < 0$ este ireductibil peste $\mathbb{R}$. Într-adevăr, dacă ar fi reductibil, s-ar putea scrie sub forma $(X - \alpha_1)(X - \alpha_2)$ cu $\alpha_1, \alpha_2 \in \mathbb{R}$, deci ar admite rădăcini reale, ceea ce nu este permis de ipoteza că $\beta^2 + 4\gamma < 0$.

Corolarul 2.5. *Orice polinom $g \in \mathbb{R}[X]$ de grad > 0 se scrie în mod unic sub forma*

$$g = \alpha(X - \alpha_1)^{e_1} \dots (X - \alpha_r)^{e_r} (X^2 - \beta_1 X - \gamma_1)^{f_1} \dots$$

$$\dots (X^2 - \beta_t X - \gamma_t)^{f_t},$$

unde $\alpha, \alpha_i, \beta_j, \gamma_j \in \mathbb{R}$, $e_i, f_j \in \mathbb{N}$, $e_i \geqslant 1$, $f_j \geqslant 1$ *şi* $\beta_j^2 + 4\gamma_j < 0$,

$$1 \leqslant i \leqslant r, \quad 1 \leqslant j \leqslant t.$$

În continuare, vom arăta că inelul $\mathbb{Z}[X]$ este factorial. Din propoziţia 1.7 rezultă că elementele ireductibile din $\mathbb{Z}[X]$ coincid cu cele prime. Se va arăta, de asemenea, că determinarea elementelor ireductibile ale inelului $\mathbb{Z}[X]$ revine la determinarea elementelor ireductibile ale inelelor $\mathbb{Z}$ şi $\mathbb{Q}[X]$. Determinarea elementelor ireductibile în $\mathbb{Z}$ şi $\mathbb{Q}[X]$ este o problemă parţial rezolvată. Cîteva rezultate privind elementele ireductibile (prime) ale lui $\mathbb{Z}$ sînt date în § 3. În acest paragraf se va da criteriul lui Eisenstein care permite evidenţierea unei întregi clase de polinoame ireductibile peste $\mathbb{Q}$.

Revenim la problema descrierii elementelor ireductibile ale inelului $\mathbb{Z}[X]$.

Lema 2.6. *Dacă p este un element prim al inelului $\mathbb{Z}$, atunci p este element prim şi al inelului $\mathbb{Z}[X]$.*

Demonstraţie. Este clar că un număr întreg $a \neq 0$ divide în inelul $\mathbb{Z}[X]$ un polinom $f \in \mathbb{Z}[X]$ dacă şi numai dacă a divide în $\mathbb{Z}$ coeficienţii polinomului f. Fie $f, g \in \mathbb{Z}[X]$,

$$f = a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0, \qquad a_m \neq 0,$$

$$g = b_n X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0, \qquad b_n \neq 0.$$

Scanned with OKEN Scanner

Presupunem că p divide în $\mathbb{Z}[X]$ polinomul fg dar p nu divide nici pe f și nici pe g în $\mathbb{Z}[X]$. Atunci există i și j astfel încît p nu divide pe a_i și nici pe b_j în inelul $\mathbb{Z}$. Fie

$$s = \min\{i \mid p \text{ nu divide } a_i\}, \quad t = \min\{j \mid p \text{ nu divide } b_j\}$$

și c_k coeficientul de indice $k = s + t$ al polinomului fg. Rezultă

$$c_k = a_s\, b_t + \sum_{\substack{i+j=k \\ i \neq s, j \neq t}} a_i\, b_j. \tag{4.2}$$

Dacă $i > s$ și $i + j = k$, atunci $j < t$. Analog, dacă $j > t$ și $i + j = k$, atunci $i < s$. Rezultă că p divide suma produselor $a_i b_j$ cu $i + j = k$, $i \neq s$, $j \neq t$. Cum p divide polinomul fg, rezultă că p divide toți coeficienții lui fg și în particular pe c_k. Din (4.2) rezultă că $p \mid a_s b_t$ și cum p este prim în $\mathbb{Z}$, rezultă că $p \mid a_s$ sau $p \mid b_t$, ceea ce contrazice definiția numerelor s și t. Rămîne adevărat că p este element prim al inelului $\mathbb{Z}[X]$.

Din lema 2.6 rezultă imediat :

Corolarul 2.7. *Polinoamele ireductibile de gradul* 0 *ale inelului* $\mathbb{Z}[X]$ *sînt exact numerele prime* p *ale inelului* $\mathbb{Z}$.

Dacă $f = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0$ este polinom din $\mathbb{Z}[X]$, cel mai mare divizor comun în $\mathbb{Z}$ al coeficienților $a_0, a_1, \ldots, a_m$, notat cu $c(f)$, se numește *conținutul lui* f. Așadar :

$$c(f) \overset{\text{def}}{=} (a_0, a_1, \ldots, a_m).$$

Polinomul f se numește *primitiv* dacă $c(f) = 1$. Astfel, conținutul polinomului $f = 6X^3 - 15X + 12$ este $c(f) = (12, -15, 6) = 3$ iar polinomul $g = 5X^2 - 3X + 12$ este primitiv, întrucît $c(g) = (12, -3, 5) = 1$.

Dacă $a \in \mathbb{Z}$, $a \neq 0$, iar $f = a_m X^m + \ldots + a_1 X + a_0$, din

$$(aa_0, aa_1, \ldots, aa_m) = a(a_0, a_1, \ldots, a_m)$$

rezultă că $c(af) = ac(f)$. Să mai observăm că

$$c(f) \mid a_i, \quad 0 \leqslant i \leqslant m,$$

Scanned with OKEN Scanner

și dacă $a_i = a_i^* \cdot c(f)$, $0 \leqslant i \leqslant m$, iar $f^* = a_m^* X^m + \ldots$ $\ldots + a_1^* X + a_0^*$, atunci

$$f = c(f)f^* \text{ și } c(f^*) = 1.$$

Lema 2.8 (*Gauss*). *Dacă f și g sînt polinoame din inelul $\mathbb{Z}[X]$, atunci :*

1) *dacă f și g sînt primitive, fg este primitiv ;*

2) $c(fg) = c(f)c(g)$.

Demonstrație. 1) Fie $c(f) = 1 = c(g)$ și $c(fg) \neq 1$. Atunci $c(fg)$ admite un divizor prim p (vezi propoziția 1.2). Cum $c(fg) \mid fg$, rezultă că $p \mid fg$ și, conform lemei 2.6, rezultă $p \mid f$ sau $p \mid g$. Dar atunci $p \mid c(f)$ sau $p \mid c(g)$, ceea ce este absurd, deoarece $c(f) = c(g) = 1$ și $p > 1$. Rămîne adevărat că $c(fg) = 1$, deci fg este polinom primitiv.

2) Fie f^* și $g^* \in \mathbb{Z}[X]$ astfel încît $f = c(f)f^*$ și $g = c(g)f^*$. Cum f^* și g^* sînt polinoame primitive, atunci de la punctul 1) rezultă că f^*g^* este primitiv. Deci :

$$c(fg) = c(c(f)c(g)f^*g^*) = c(f)c(g)c(f^*g^*) = c(f)c(g).$$

Lema 2.9. *Fie $f, g \in \mathbb{Z}[X]$, $a \in \mathbb{Z}$, $a \neq 0$, și f primitiv. Dacă f divide ag în inelul $\mathbb{Z}[X]$, atunci f divide g în inelul $\mathbb{Z}[X]$.*

Demonstrație. Fie $h \in \mathbb{Z}[X]$ astfel încît $ag = fh$ și fie $g^*, h^* \in \mathbb{Z}[X]$ astfel încît $g = c(g)g^*$ și $h = c(h)h^*$. Avem

$$c(h) = c(fh) = c(ag) = ac(g),$$

de unde $g^* = fh^*$. Deci $f \mid g^*$ și cum $g^* \mid g$, rezultă $f \mid g$.

Următoarea teoremă descrie polinoamele ireductibile de grad $\geqslant 1$ din inelul $\mathbb{Z}[X]$.

Teorema 2.10. *Fie f un polinom din $\mathbb{Z}[X]$ de grad $\geqslant 1$. Următoarele afirmații sînt echivalente :*

1) *f este element ireductibil al inelului $\mathbb{Z}[X]$.*

2) *f este primitiv și ireductibil peste $\mathbb{Q}$.*

Scanned with OKEN Scanner

Demonstrație. 1) $\Rightarrow$ 2). Avem $f = c(f)f^*$ cu $\deg(f^*) = \deg(f) > 1$. Rezultă că f^* nu poate fi o unitate a inelului $\mathbb{Z}[X]$. Cum f este element ireductibil al inelului $\mathbb{Z}[X]$ din $f = c(f)f^*$, rezultă că $c(f)$ este unitate în $\mathbb{Z}[X]$. Dar unitățile lui $\mathbb{Z}[X]$ sînt ± 1, deci $c(f) = 1$ și f este primitiv.

Dacă f este reductibil peste $\mathbb{Q}$, există două polinoame $g, h \in \mathbb{Q}[X]$, de grad strict mai mic ca gradul lui f, astfel încît $f = gh$. Coeficienții lui g și h sînt fracții de elemente din $\mathbb{Z}$. Este clar că există $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ astfel încît polinoamele $g_1 = ag$ și $h_1 = bh$ să aibă coeficienții întregi. Fie $g_1^*, h_1^* \in \mathbb{Z}[X]$ astfel încît $g_1 = c(g_1)g_1^*$ și $h_1 = c(h_1)h_1^*$. Atunci

$$abf = abgh = g_1h_1 = c(g_1)c(h_1)g_1^*h_1^*,$$

de unde, ținînd seama că f, g_1^* și h_1^* sînt polinoame primitive, obținem

$$f = g_1^*h_1^*.$$

Cum $\deg(g) = \deg(g_1) = \deg(g_1^*)$ și $\deg(h) = \deg(h_1) = \deg(h_1^*)$, rezultă că f este produs de polinoame din $\mathbb{Z}[X]$, ambele de grad strict mai mic ca cel al lui f. Deci, f este reductibil în $\mathbb{Z}[X]$, ceea ce contrazice ipoteza făcută asupra lui f. Rămîne adevărat că f este ireductibil peste $\mathbb{Q}$. Din 2) rezultă 1). De aici se obține

Corolar 2.11. *Elementele ireductibile ale inelului $\mathbb{Z}[X]$ sînt polinoamele constante p (p fiind număr întreg prim) și polinoamele primitive de grad $\geqslant 1$ care sînt ireductibile peste $\mathbb{Q}$.*

Observație. Dacă $g \in \mathbb{Z}[X]$ are gradul >0, atunci g este reductibil peste $\mathbb{Z}$ dacă și numai dacă poate fi reprezentat ca produs de două polinoame din $\mathbb{Z}[X]$, ambele de grad strict mai mic ca gradul lui g.

Lema 2.12. *Orice element ireductibil f din $\mathbb{Z}[X]$ este prim.*

Demonstrație. Dacă f este polinom de gradul 0, atunci f este evident element ireductibil și al inelului $\mathbb{Z}$. Cum $\mathbb{Z}$ este euclidian, $f = p$, unde p este un număr întreg prim

Scanned with OKEN Scanner

(vezi propoziția 1.4). Conform lemei 2.6, acesta este element prim al inelului $\mathbb{Z}[X]$. Dacă $\deg(f)>0$, atunci, conform teoremei 2.10, f este primitiv și ireductibil peste $\mathbb{Q}$. Fie g și $h \in \mathbb{Z}[X]$ astfel încît $f \mid gh$. Trebuie arătat că $f \mid g$ sau $f \mid h$ în inelul $\mathbb{Z}[X]$. Cum f este ireductibil peste $\mathbb{Q}$, din $f \mid gh$ rezultă $f \mid g$ sau $f \mid h$ în inelul $\mathbb{Q}[X]$. Fie $f \mid g$ în $\mathbb{Q}[X]$. Există $g_1 \in \mathbb{Q}[X]$ astfel încît $g = fg_1$ și $a \in \mathbb{Z}$, $a \neq 0$, astfel încît $g_2 = ag_1 \in \mathbb{Z}[X]$. Avem $ag = fg_2$, de unde rezultă că $f \mid ag$ în inelul $\mathbb{Z}[X]$. Conform lemei 2.9, $f \mid g$ în inelul $\mathbb{Z}[X]$. La fel se arată dacă $f \mid h$ în inelul $\mathbb{Q}[X]$, atunci $f \mid h$ în inelul $\mathbb{Z}[X]$ și lema este demonstrată.

Teorema 2.13. *Inelul $\mathbb{Z}[X]$ este factorial.*

Demonstrație. Fie $g \in \mathbb{Z}[X]$, nenul și neinversabil ($g \neq \pm 1$). Arătăm mai întîi că g este produs finit de polinoame ireductibile peste $\mathbb{Z}$. Dacă $\deg(g) = 0$, atunci g este un număr întreg, deci g este produs finit de numere prime care sînt polinoame ireductibile ale lui $\mathbb{Z}[X]$ (vezi corolarul 2.11). Presupunem că $\deg(g)>0$. Dacă g este ireductibil peste $\mathbb{Z}$, nu mai este nimic de demonstrat. Presupunem că g este reductibil peste $\mathbb{Z}$. Atunci există polinoamele h_1, $h_2 \in \mathbb{Z}[X]$ astfel încît

$$g = h_1h_2, \quad \deg(h_1)<\deg(g), \quad \deg(h_2)<\deg(g).$$

Presupunînd afirmația adevărată pentru polinoame de grad $<\deg(g)$, rezultă că h_1 și h_2 sînt produse finite de polinoame ireductibile peste $\mathbb{Z}$, deci și $g = h_1h_2$ are aceeași proprietate. Unicitatea descompunerii în factori ireductibili (primi) în inelul $\mathbb{Z}[X]$ se demonstrează analog cu teorema 1.5, avînd în vedere lema 2.12.

Propunem cititorului să arate că inelul $\mathbb{Z}[X]$ nu este euclidian.

Teorema 2.14 (*criteriul lui Eisenstein*). *Fie $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ un polinom cu coeficienți întregi, $a_n \neq 0$, $n>1$. Presupunem că există un număr prim p astfel încît $p \mid a_i$, $0 \leqslant i<n$, p nu divide a_n și p^2 nu divide a_0. Atunci f este ireductibil peste $\mathbb{Q}$.*

Scanned with OKEN Scanner

Demonstrație. Cum $c(f)$ este element inversabil în inelul $\mathbb{Q}[X]$ și $f = c(f)\, f^*$ cu f primitiv, rezultă că f și f^* sînt asociați în divizibilitate în inelul $\mathbb{Q}[X]$, deci simultan ireductibili sau reductibili peste $\mathbb{Q}$. Așadar, putem presupune că f este primitiv. Dacă f este reductibil peste $\mathbb{Q}$, atunci f este reductibil și peste $\mathbb{Z}$ (vezi teorema 2.10). Atunci există două polinoame $g, f \in \mathbb{Z}[X]$:

$$g = b_0 + b_1X + \ldots + b_s X^s, \quad h = c_0 + c_1X + \ldots + c_tX^t$$

cu $s<n$ și $t<n$ astfel încît $f = gh$. Deoarece $a_0 = b_0c_0$ și $p \mid a_0$ dar p^2 nu divide a_0, rezultă că $p \mid b_0$ și p nu divide c_0 sau p nu divide b_0 și $p \mid c_0$. Pentru a face o alegere, presupunem că $p \mid b_0$ și p nu divide c_0. Putem defini:

$$k = \min \{i \mid p \text{ nu divide } b_i\}$$

și avem $1<k\leqslant s<n$. Cum

$$a_k = b_kc_0 + \sum_{i=0}^{k-1} b_i\, c_{k-1}$$

și $k<n$, avem $p \mid a_k$. Pentru $i<k$ de asemenea $p \mid b_i$ și atunci din egalitatea precedentă rezultă că $p \mid b_kc_0$ cu toate că p nu divide pe b_k și nici pe c_0. (contradicție !). Rezultă că f este ireductibil peste $\mathbb{Q}$.

Observație. Am văzut că polinoamele ireductibile peste $\mathbb{C}$ au gradul întîi iar cele peste $\mathbb{R}$ au gradul cel mult 2. Totuși, pentru orice n există un polinom ireductibil peste $\mathbb{Q}$ de grad n. Într-adevăr, dacă p este număr prim, atunci polinomul $f = X^n - p$ este, conform criteriului lui Eisenstein, ireductibil peste $\mathbb{Q}$.

§ 3. Metode algoritmice pentru descompunerea numerelor în factori primi

În cap. II am demonstrat că orice număr natural $n>1$ poate fi reprezentat în mod unic ca produs de numere prime:

$$n = p_1p_2 \ldots p_r, \quad p_1\leqslant p_2\leqslant \ldots \leqslant p_r.$$

Scanned with OKEN Scanner

Demonstrația acestui rezultat nu oferă și o metodă cu ajutorul căreia să putem găsi descompunerea în factori primi a numerelor naturale.

Să observăm că în descompunerea în factori primi a unui număr natural $n>1$ apar numere prime $\leqslant n$. O eventuală metodă de descompunere a numerelor naturale în factori primi va opera deci pentru orice $n>1$ cu tabla numerelor prime $\leqslant n$. O metodă de a întocmi tabla numerelor naturale prime mai mici ca un număr natural dat n a fost dată încă din antichitate și este cunoscută sub denumirea de *ciurul lui Eratostene* (275—195 î.e.n.). Pe scurt, metoda constă din următoarele:

1° se scrie șirul numerelor naturale de la 1 la n;

2° se înlătură din șir numărul 1, care nu este prim;

3° se înlătură apoi din șir (după o procedură ce va fi dată mai jos) toate numerele m ce sînt multipli de numere naturale c, $1<c<m$.

Numerele rămase după ce efectuăm 1°, 2° și 3° sînt exact numerele prime $p\leqslant n$. Într-adevăr, cum, evident, prin 2° și 3° nu se elimină numere prime, este suficient să arătăm că orice „supraviețuitor" p este prim. Datorită lui 2°, orice $p>1$. Rezultă că dacă p nu este prim, atunci există un întreg c, $1<c<p$, astfel încît $c \mid p$, ceea ce nu se poate, întrucît atunci p ar fi fost „victima" lui 3°.

Înainte de a redacta metoda ciurului lui Eratostene în termenii unui algoritm, dăm cîteva rezultate simple.

Propoziția 3.1. *Dacă $n>1$ este un număr natural care nu este prim, atunci n admite un divizor d astfel încît $1<d\leqslant\sqrt{n}$.*

Demonstrație. Cum n nu este prim, există două numere naturale a și b astfel încît

$$n = ab,\ 1<a<n,\ 1<b<n.$$

Putem presupune că $a\leqslant b$ și avem

$$1<a^2\leqslant ab = n,$$

de unde $1<a\leqslant\sqrt{n}$. Se ia $d = a$ și rezultă afirmația din propoziție.

Scanned with OKEN Scanner

Corolarul 3.2. *Orice număr natural $n>1$ care nu este prim admite un divizor prim p astfel încît $p \leqslant \sqrt{n}$.*

Demonstrație. Fie d un divizor al lui n astfel încît $1<d\leqslant\sqrt{n}$ (vezi propoziția 3.1). Orice divizor prim p al lui d satisface cerința din enunț.

Iată acum metoda ciurului lui Eratostene prezentată sub forma unui algoritm :

P_1. Scrie numerele naturale de la 1 la n.

P_2. Elimină numărul 1.

P_3. Găsește cel mai mic număr p dintre numerele neeliminate.

P_4. Dacă $p>\sqrt{n}$, treci la P_6.

P_5. Elimină dintre numerele rămase toți multiplii lui p strict mai mari ca p și treci la P_3.

P_6. STOP

Algoritmul ne dă în final tabla tuturor numerelor prime $\leqslant n$. Într-adevăr, numerele p determinate la P_3 sînt prime, deoarece nu admit divizori primi mai mici ca p (altfel ar fi fost eliminate în etapele precedente). Din listă sînt eliminate numai numere ce nu sînt prime (prin P_1 și P_5). După ce se parcurge ciclul $P_3\to P_4\to P_5\to P_3$ de un număr finit de ori ($\leqslant[\sqrt{n}]$), se ajunge la instrucțiunea P_6, moment în care lista de numere rămase constă exact din numerele prime $\leqslant n$. Într-adevăr, în momentul cînd realizăm prima dată $p>\sqrt{n}$, orice număr m rămas în listă este prim ; în caz contrar m nu admite un divizor prim q, $q\leqslant\sqrt{m}$ (vezi corolarul 3.2). Deci

$$q\leqslant\sqrt{m}\leqslant\sqrt{n}<p.$$

Dar m este eliminat prin P_5 imediat ce realizăm q cu P_3 (evident înaintea lui p).

Astfel, dacă $n = 100$, atunci $[\sqrt{100}] = 10$. Prin P_3 se determină succesiv numerele prime

2, 3, 5, 7, 11.

Cum $11 > [\sqrt{100}]$, operația de „curățire" a secvenței

$$1, 2, 3, 4, \ldots, 99, 100$$

de numere ce nu sînt prime este terminată.

Numerele prime $\leqslant 100$ sînt

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 51, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Lista de numere prime nu lasă să se întrevadă vreo regulă privind distribuția numerelor prime printre numerele naturale. Rezultate profunde privind distribuția numerelor prime au, de regulă, demonstrații ce depășesc nivelul acestei cărți. Pentru următorul rezultat există o demonstrație elementară.

Propoziția 3.3. *Dacă n este un număr natural >2, atunci există un număr prim p astfel încît*

$$n < p < n\,!.$$

Demonstrație. Cum $n > 2$, avem $n\,! - 1 > 1$, deci $n\,! - 1$ admite un divizor prim p. Dacă $p \leqslant n$, atunci $p \mid n\,!$ și cum $p \mid (n\,! - 1)$, rezultă că $p \mid 1$ (contradicție !). Așadar, $n < p$. Pe de altă parte, $p \leqslant n\,! - 1 < n\,!$, deci $n < p < n\,!$.

Din propoziția precedentă rezultă că pentru orice număr natural $n > 2$ există un număr prim p mai mare ca n. În particular, pentru orice număr prim p, există un număr prim q astfel încît $p < q$. Acum rezultă imediat că mulțimea numerelor prime este infinită (vezi, de asemenea, corolarul 2.9, cap. II). Are sens deci să ne punem problema următoare: pentru un număr natural m să se determine primele m numere prime. Au fost întocmite tabele cu primele m numere prime, cu m de ordinul milioanelor. Acest lucru este important în studiul cu mijloace statistice ale numerelor prime.

Pe calculatoare electronice cu memorie suficient de cuprinzătoare se pot întocmi tabele cu primele m numere naturale prime, cu m foarte mare. Pentru a încredința unui calculator o asemenea sarcină este necesar să dis-

punem de un algoritm prin care să organizăm munca acestuia. Vom prezenta un algoritm pentru întocmirea tabelelor cu primele m numere prime. Avem în acest scop nevoie de un rezultat care ameliorează pe cel din teorema 3.3, rezultat cunoscut sub denumirea de postulatul lui Bertrand, demonstrat de către Cebîșev în 1850. Propunem cititorului să-l accepte fără demonstrație.

Teorema 3.4 (*Bertrand*). *Pentru orice număr natural* $n>1$ *există un număr prim* p *astfel încît* $n<p<2n$.

Vom mai folosi și rezultatele de mai jos.

Lema 3.5. *Fie* $n>1$ *și* p *un număr prim astfel încît:*

$$n = pq + r, \quad 0<r<p, \quad q \leqslant p.$$

Dacă n *nu admite divizori primi mai mici ca* p, *atunci* n *este prim.*

Demonstrație. Avem $n = pq + r < p^2 + p < (p+1)^2$. Dacă n nu este prim, atunci n admite un divizor prim $p_1 \leqslant \sqrt{n} < p+1$ (vezi corolarul 3.2). Avem $p_1 \leqslant p$ și cum p nu divide n, rezultă $p_1 < p$, contrar ipotezei din enunț. Rămîne adevărat că n este prim.

Teorema 3.6. *Fie* $p_1, p_2, \ldots, p_h, p$ *primele* $h+1$ *numere naturale prime,* $p_1 < p_2 < \ldots < p_h < p$, $h>1$.

1) *Pentru orice* i, $0 < i < (p - p_h)/2$, *există* k_i, $1 \leqslant k_i \leqslant h$, *astfel încît*

$$(p_h + 2i) \bmod p_k \neq 0, \left[\frac{p_h + 2i}{p_h}\right] > p_k, \quad 1 \leqslant k < k_i,$$

și

$$(p_h + 2i) \bmod p_{k_i} = 0.$$

2) *Există* k_0, $1 \leqslant k_0 \leqslant h$, *astfel încît*

$$\left[\frac{p}{p_k}\right] > p_k, \; 1 \leqslant k < k_0,$$

Scanned with OKEN Scanner

Scanned with OKEN Scanner

și

$$\left[\frac{p}{p_{k_0}}\right] \leqslant p_{k_0}.$$

Mai mult, $p \bmod p_k \neq 0$, $1 \leqslant k \leqslant h$.

Demonstrație. 1) Întrucît p_h și p sînt numere prime consecutive și $p_h < p_h + 2i < p$, rezultă că $p_h + 2i$ nu este prim. Atunci $p_h + 2i$ admite un divizor prim mai mic decît $p_h + 2i$. Cum numerele prime mai mici ca $p_h + 2i$ sînt $p_1, p_2, \ldots, p_h$, rezultă că mulțimea

$$P = \{k \mid 1 \leqslant k \leqslant h, (p_h + 2i) \bmod p_k = 0\}$$

nu este vidă. Dacă k_i este cel mai mic număr din P, atunci pentru $0 \leqslant k < k_i$ rezultă

$$p_h + 2i = p_k q_k + r_k, \quad 0 < r_k < p_k.$$

De asemenea $q_k > p_k$, deoarece altfel $q_k \leqslant p_k$ și $r_k \neq 0$ implică faptul că $p_h + 2i$ este prim (vezi lema 3.5), ceea ce nu este adevărat.

Așadar

$$\left[\frac{p_h + 2i}{p_k}\right] > p_k, \quad 1 \leqslant k < k_i,$$

și 1) este demonstrat.

2) Întrucît p este prim, rezultă că $p \bmod p_k \neq 0$, $1 \leqslant k \leqslant h$. În particular, $p \bmod p_h \neq 0$, deci există $q_h, r_h \in \mathbb{N}$, astfel încît

$$p = p_h q_h + r_h, \quad 0 < r_h < p_h.$$

Cum $h > 1$, rezultă $p_h \geqslant 3$ iar conform teoremei 3.4 rezultă și $p_h < p < 2p_h$. Se deduce că

$$q_h = \frac{p - r_h}{p_h} < \frac{p}{p_h} < \frac{2p_h}{p_h} = 2 < p_h,$$

de unde rezultă că mulțimea

$$M = \left\{k \mid 1 \leqslant k \leqslant h, \left[\frac{p}{p_h}\right] \leqslant p_k\right\}$$

este nevidă, fiindcă $h \in M$. Afirmația 2) din enunțul teoremei se verifică luînd k_0 egal cu cel mai mic număr din M.

Algoritmul propus în cele ce urmează conduce la aflarea primelor m numere prime $p_1 < p_2 < \ldots < p_m$, $m > 1$. Într-adevăr, utilizînd variabilele k, l, n și q, instrucțiunile algoritmului sînt următoarele:

T_1. $p_1 \leftarrow 2$, $n \leftarrow 3$, $l \leftarrow 1$.

T_2. $l \leftarrow l + 1$, $p_l \leftarrow n$.

T_3. Dacă $l = m$, treci la T_{10}.

T_4. $n \leftarrow n + 2$.

T_5. $k \leftarrow 2$.

T_6. Dacă $p_k \mid n$, treci la T_4.

T_7. $q \leftarrow \left[\frac{n}{p_k}\right]$.

T_8. Dacă $q \leqslant p_k$, mergi la T_2.

T_9. $k \leftarrow k + 1$ și mergi la T_6.

T_{10}. STOP.

Schema logică a acestui algoritm este dată la fig. 12.

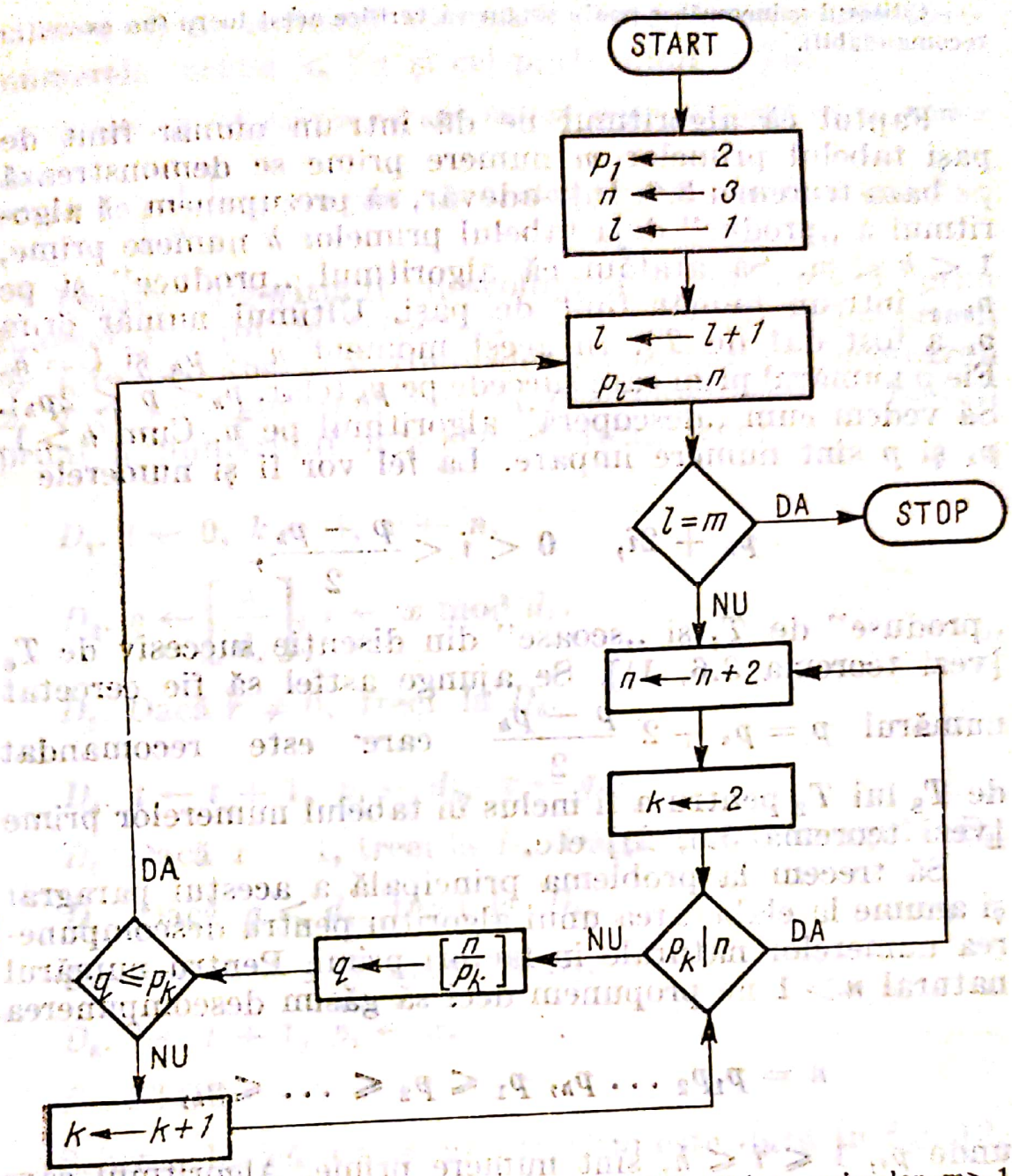


Fig. 12. Schema logică a algoritmului pentrû găsirea primelor $m > 1$ numere prime.

Să vedem la lucru algoritmul elaborat în cazul $m = 7$. Vor fi găsite primele șapte numere prime, deci numerele 2, 3, 5, 7, 11, 13 și 17. În acest caz instrucțiunile algoritmului se execută ca în secvența ce urmează:

$$T_1 \to T_2 \to T_3 \to T_4 \to T_5 \to T_6 \to T_7 \to T_8 \to T_2 \to T_3 \to T_4 \to T_5 \to T_6 \to T_7 \to$$
$$\to T_8 \to T_2 \to T_3 \to T_4 \to T_5 \to T_6 \to T_4 \to T_5 \to T_6 \to T_7 \to T_8 \to T_2 \to T_3 \to$$
$$\to T_4 \to T_5 \to T_6 \to T_7 \to T_8 \to T_9 \to T_6 \to T_7 \to T_8 \to T_2 \to T_3 \to T_4 \to T_5 \to T_6 \to T_4 \to$$
$$\to T_5 \to T_6 \to T_7 \to T_8 \to T_9 \to T_6 \to T_7 \to T_8 \to T_2 \to T_3 \to T_{10}.$$

Cititorul neîncrezător poate singur să verifice acest lucru (un exercițiu recomandabil).

Faptul că algoritmul ne dă într-un număr finit de pași tabelul primelor m numere prime se demonstrează pe baza teoremei 3.6. Într-adevăr, să presupunem că algoritmul a „produs" deja tabelul primelor h numere prime, $1 < h < m$. Să arătăm că algoritmul „produce" și pe p_{h+1} într-un număr finit de pași. Ultimul număr prim p_h a fost dat de T_2. În acest moment $n = p_h$ și $l = h$. Fie p numărul prim care succede pe p_h (clar, $p_h < p < 2p_h$). Să vedem cum „descoperă" algoritmul pe p. Cum $h > 1$, p_h și p sînt numere impare. La fel vor fi și numerele

$$p_h + 2i, \quad 0 < i < \frac{p - p_h}{2},$$

„produse" de T_4 și „scoase" din discuție succesiv de T_6 [vezi teorema 3.6, 1)]. Se ajunge astfel să fie cercetat numărul $p = p_h + 2\,\frac{p - p_h}{2}$ care este recomandat de T_8 lui T_2 pentru a fi inclus în tabelul numerelor prime [vezi teorema 3.6, 2)] etc.

Să trecem la problema principală a acestui paragraf și anume la elaborarea unui algoritm pentru descompunerea numerelor naturale în factori primi. Pentru numărul natural $n > 1$ ne propunem deci să găsim descompunerea

$$n = p_1 p_2 \ldots p_h, \; p_1 \leqslant p_2 \leqslant \ldots \leqslant p_h,$$

unde p_i, $1 \leqslant i \leqslant h$, sînt numere prime. Algoritmul care va fi dat are ca operație de bază împărțirea cu rest prin numerele prime

$$2, \; 3, \; 5, \; 7, \ldots$$

Se va folosi deci o listă de divizori „de încercare" care constă din tabelul primelor numere prime

$$2 = d_1 < d_2 < \ldots$$

Scanned with OKEN Scanner

și care să fie suficient de mare pentru a cuprinde toate numerele prime $\leqslant \sqrt{n}$ și cel puțin unul $> \sqrt{n}$.

Reamintim că dacă n nu are divizori primi mai mici ca un număr prim p iar $\left[\frac{n}{p}\right] \leqslant p$ și $n \bmod p \neq 0$, atunci n este prim (vezi lema 3.5).

Pentru algoritmul descompunerii în factori prim folosim variabilele t (pentru indexarea factorilor primi, de cîte ori apar), k (indicele divizorului de încercare), x, q și r. Algoritmul pentru descompunerea în factori primi a numărului $n > 1$ este următorul:

D_1. $t \leftarrow 0$, $k \leftarrow 1$, $x \leftarrow n$.

D_2. $q \leftarrow \left[\frac{x}{d_k}\right]$, $r \leftarrow x \bmod d_k$.

D_3. Dacă $r \neq 0$, treci la D_6.

D_4. $t \leftarrow t + 1$, $p_t \leftarrow d_k$, $x \leftarrow q$.

D_5. Dacă $x = 1$, treci la D_9. Dacă $x \neq 1$, mergi la D_2.

D_6. Dacă $q \leqslant d_k$, treci la D_8.

D_7. $k \leftarrow k + 1$ și mergi la D_2.

D_8. $t \leftarrow t + 1$, $p_t \leftarrow x$.

D_9. STOP.

Schema logică a acestui algoritm este dată în fig. 13.

Dacă la D_3 avem $r \neq 0$ și la D_6 avem $q \leqslant d_k$, atunci $x = d_k q + r$ este, conform lemei 3.5, număr prim și x va fi ultimul factor prim al lui n (vezi instrucțiunea D_8). În rest, acțiunea algoritmului este evidentă.

Să urmărim cum acționează acest algoritm cînd $n = 847$. Cum $[\sqrt{847}] = 29$, lista divizorilor de încercare în acest caz poate cuprinde doar numerele prime

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

Scanned with OKEN Scanner

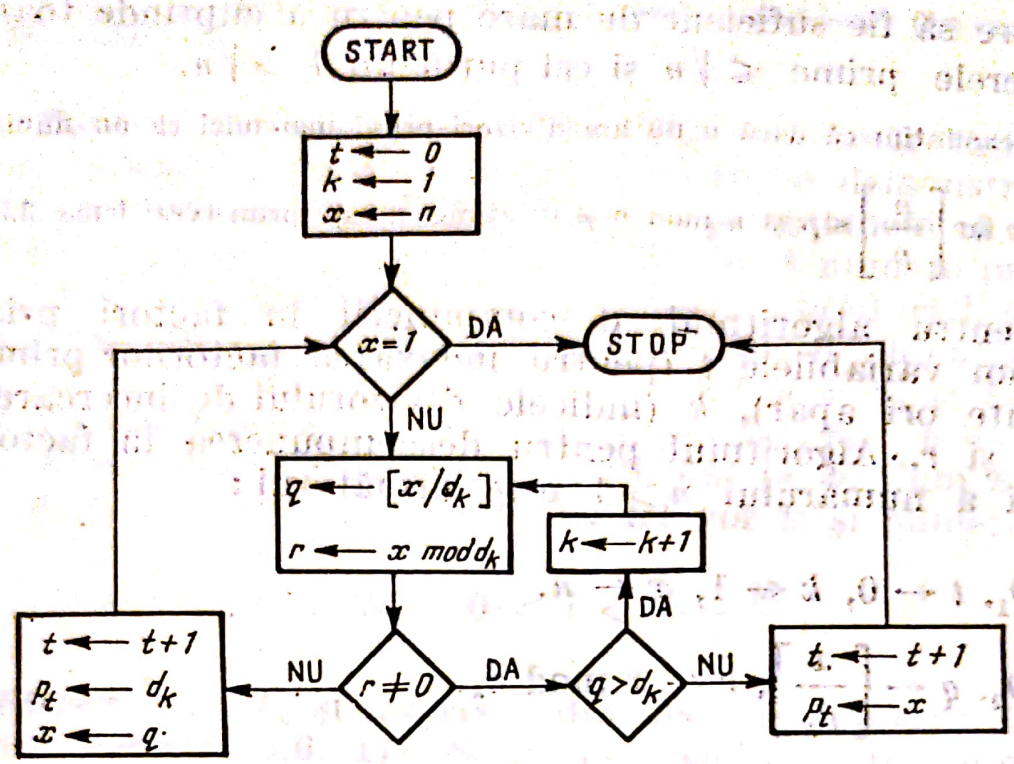


Fig. 13. Schema logică a algoritmului descompunerii în factori primi.

În tabelul 7 sînt date valorile variabilelor t, k, x, q, r, precum și factorii primi $p_1, p_2, \ldots, p_h$ ai lui n. Avem $d_1 = 2$, $d_2 = 3, \ldots, d_{11} = 31$. Rezultă că $h = 3$, $p_1 = 7$, $p_2 = 11$, $p_3 = 11$, deci

$$847 = 7 \times 11 \times 11.$$

Propunem cititorului să găsească secvența de instrucțiuni care conduce la această descompunere.

t	k	x	q	r	p_t
0	1	847	423	1	—
0	2	847	282	1	—
0	3	847	169	2	—
1	4	847	121	0	7
1	1	121	60	1	—
1	2	121	40	1	—
1	3	121	24	1	—
1	4	121	17	2	—
2	5	121	11	0	11
2	1	11	5	1	—
2	2	11	3	2	11

Tabelul 7

Scanned with OKEN Scanner

Observăm că un număr natural n admite ca divizor pe 2 cu probabilitatea $\frac{1}{2}$, pe 3 cu probabilitatea $\frac{1}{3}$, pe 5 cu probabilitatea $\frac{1}{5}$ etc. Aşadar, probabilitatea ca un număr natural n să admită divizori primi mari este mică.

Algoritmul precedent găseşte divizorii primi mici după un volum relativ mic de calcule. În schimb, acest algoritm este foarte lent cînd n admite divizori primi foarte mari. Pornind de la o metodă a lui Fermat de a găsi divizorii mari ai numerelor naturale, se atenuează inconvenientul menţionat al algoritmului dat.

Folosind o variantă evidentă a algoritmului precedent, se poate pune numărul natural n sub forma

$$n = 2^r m, \quad r \geqslant 0, \quad (2, m) = 1.$$

Aşadar, putem presupune că n este impar.

Vom elabora un algoritm pentru găsirea celui mai mare divizor d al lui n, astfel încît $d \leqslant \sqrt{n}$. În acest sens, vom investiga produsele uv, cu u şi v numere naturale, $u \leqslant v$, astfel încît cantitatea

$$r = uv - n$$

să „oscileze" în jurul lui 0. Căutăm să realizăm $n = uv$ (deci $r = 0$), astfel încît u şi v să fie cît mai apropiaţi, ceea ce, împreună cu condiţia $u \leqslant v$, va da pe cel mai mare divizor d al lui n astfel încît $d \leqslant \sqrt{n}$. Cum n este presupus impar, egalitatea $n = uv$ (deci $r = 0$) are loc pentru u şi v impari. Pentru a avea mai multă libertate, studiem oscilaţia cantităţii $r = uv - n$ în jurul lui 0 pentru u şi v de aceeaşi paritate (ambele pare sau ambele impare) cu $u \leqslant v$. Dacă u şi v au aceeaşi paritate şi $u \leqslant v$, atunci

$$x = \frac{u+v}{2}, \quad y = \frac{v-u}{2}$$

sînt întregi $\geqslant 0$ şi avem chiar $0 \leqslant y < x$. Cînd $uv = n$, avem $0 \leqslant y < x \leqslant n$. Se poate scrie

$$uv = (x-y)(x+y) = \frac{x'-y'}{2} \cdot \frac{x'+y'-2}{2},$$

unde $x' = 2x + 1$, $y' = 2y + 1$.

Scanned with OKEN Scanner

Să observăm că dacă u și v sînt pare, atunci $u+1$ și $v+1$ sînt impare și la fel $u-1$ și $v+1$ sînt impare. Dacă u și v sînt impare, atunci $u+1$ și $v+1$ sînt pare și la fel $u-1$ și $v+1$ sînt pare.

De la cuplul u și v se trece la cuplul $u+1$, $v+1$, prin substituția

$$x' \leftarrow x' + 2 \qquad (4.3)$$

iar de la cuplul u, v la cuplul $u-1$, $v+1$ se trece prin substituția

$$y' \leftarrow y' + 2.$$

Se observă că $x' \leftarrow x' + 2$ atrage $r \leftarrow r + x'$ iar $y' \leftarrow y' + 2$ atrage $r \leftarrow r - y'$. În concluzie, substituția $x' \leftarrow x' + 2$ crește valoarea lui r, iar $y' \leftarrow y' + 2$ scade valoarea lui r, ambele substituții menținînd pe u și v de aceeași paritate. Se va folosi adecvat una sau alta din substituțiile (4.3) și (4.4) pentru a realiza oscilația lui r în jurul lui 0 pînă cînd se realizează prima dată $r = 0$, situație care va da divizorul lui n căutat (cel mai mare divizor d al lui n astfel încît $d \leqslant \sqrt{n}$).

Începem algoritmul prin a ne încerca șansele cu următoarele valori inițiale:

$$u \leftarrow [\sqrt{n}], \qquad v \leftarrow [\sqrt{n}],$$

ceea ce revine la

$$x \leftarrow [\sqrt{n}], \qquad y \leftarrow 0$$

sau încă la

$$x' \leftarrow 2\,[\sqrt{n}] + 1, \qquad y' \leftarrow 1.$$

Cînd n este pătrat perfect, rezultă $n = uv$, $u = v = [\sqrt{n}] = d$ și algoritmul se termină cu o soluție ideală la problema pusă. Dacă n nu este pătrat perfect, atunci $[\sqrt{n}] < \sqrt{n}$ și $[\sqrt{n}] + 1 > n$, de unde

$$r = [\sqrt{n}]^2 - n < 0.$$

Făcînd substituția (4.3), se obține

$$r \leftarrow r + x' = [\sqrt{n}]^2 + 2\,[\sqrt{n}] + 1 - n = \\ = [\sqrt{n} + 1]^2 - n > 0.$$

Scanned with OKEN Scanner

Mai departe, se operează cu (4.4) pînă se obține prima dată $r \leqslant 0$, apoi cu (4.3) pentru a obține $r \geqslant 0$ etc. pînă se obține prima dată $r = 0$. (Demonstrați că aceasta se întîmplă după un număr finit de pași!). Transformările (4.3) și (4.4) păstrează inegalitatea $u \leqslant v$. Cînd se obține prima dată $r = 0$, valoarea $d = u$ este divizor al lui n, $d \leqslant [\sqrt{n}]$, d fiind cel mai mare cu aceste proprietăți (demonstrați!).

Folosind variabilele r, x', y', algoritmul poate fi redactat astfel:

F_1. $x' \leftarrow 2\,[\sqrt{n}] + 1$, $y' \leftarrow 1$, $r \leftarrow [\sqrt{n}]^2 - n$.

F_2. Dacă r nu este > 0, treci la F_4.

F_3. $r \leftarrow r - y'$, $y' \leftarrow y' + 2$ și mergi la F_2.

F_4. Dacă $r = 0$, treci la F_6.

F_5. $r \leftarrow r + x'$, $x' \leftarrow x' + 2$ și mergi la F_2.

F_6. $d \leftarrow \dfrac{x' - y'}{2}$.

F_7. STOP.

Schema logică a acestui algoritm este dată în fig. 14.

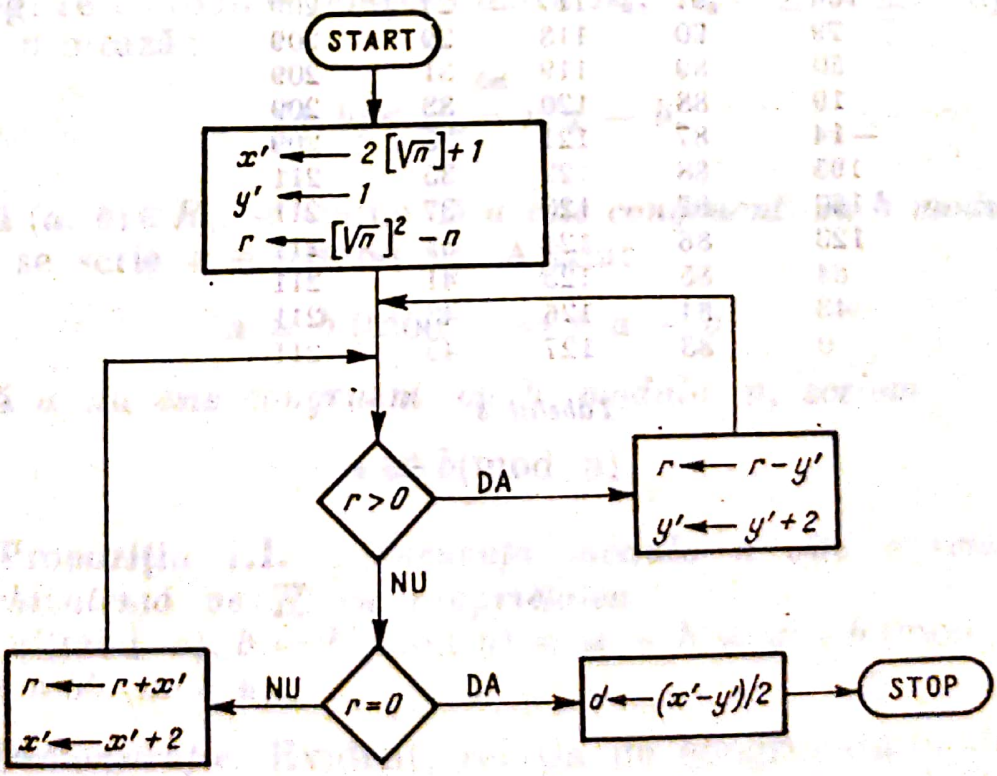


Fig. 14.

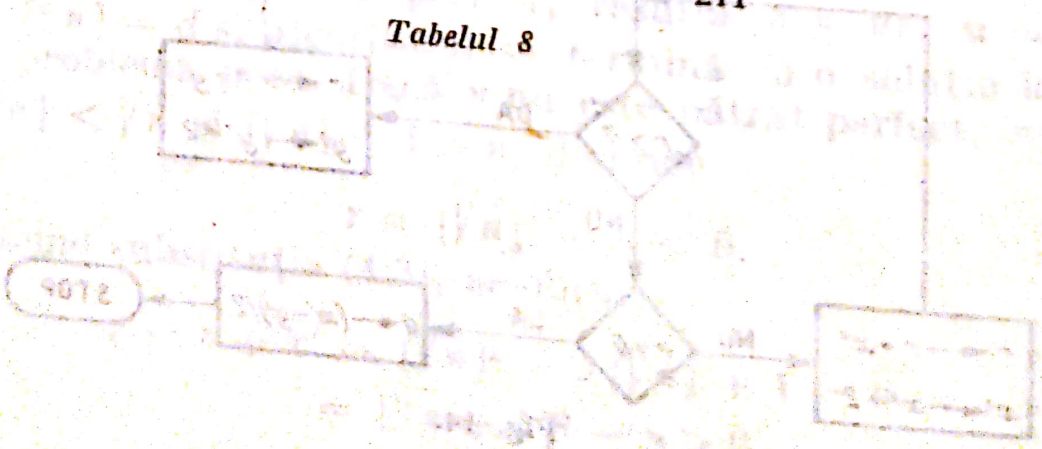
Fie $n = 10\,541$ și să găsim cel mai mare divizor d al lui n astfel încît $d \leqslant \sqrt{n}$. Avem

$$[\sqrt{n}] = [\sqrt{10\,541}] = 102.$$

În tabelul 8 sînt trecute valorile variabilelor r, u, v, y', x'. Pe linia valorii $r = 0$ avem $u = 83$ și $v = 127$. Numărul căutat este $d = 83$.

r	u	v	y'	x'
−137	102	102	1	205
68	103	103	1	207
67	102	104	3	207
64	101	105	5	207
59	100	106	7	207
52	99	107	9	207
43	98	108	11	207
32	97	109	13	207
19	96	110	15	207
4	95	111	17	207
−13	94	112	19	107
194	95	113	19	209
175	94	114	21	209
154	93	115	23	209
131	92	116	25	209
106	91	117	27	209
79	90	118	29	209
50	89	119	31	209
19	88	120	33	209
−14	87	121	35	209
195	88	122	35	211
160	87	123	37	211
123	86	124	39	211
84	85	125	41	211
43	84	126	43	211
0	83	127	45	211

Tabelul 8



CAPITOLUL V

Aritmetică modulară

§ 1. Inelul claselor de resturi modulo n

Fie n un număr întreg pozitiv. Pe inelul $\mathbb{Z}$ al numerelor întregi se introduce relaţia binară R_n, $R_n \subset \mathbb{Z} \times \mathbb{Z}$, după cum urmează:

$$(a, b) \in R_n \overset{\text{def}}{\Leftrightarrow} n \mid a - b.$$

Dacă $(a, b) \in R_n$, se spune că *a este congruent cu b modulo n* şi se scrie $a \equiv b \pmod{n}$. Aşadar

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b.$$

Dacă *a nu este congruent cu b modulo n*, scriem

$$a \not\equiv b \pmod{n}.$$

Propoziţia 1.1. *Congruenţa modulo n este o relaţie de echivalenţă pe $\mathbb{Z}$ cu proprietatea* $a = a' \pmod{n}$, $b = b' \pmod{n} \Rightarrow a + b = a' + b' \pmod{n}$, $ab = a'b' \pmod{n}$.

Demonstraţie. Evident, relaţia de congruenţă modulo n este reflexivă şi simetrică. Dacă $a \equiv b \pmod{n}$ şi

Scanned with OKEN Scanner

$b \equiv c \pmod{n}$, atunci $a - n = nh$ şi $b - c = nk$ cu $h, k \in \mathbb{Z}$. Deci $a - c = (a - b) + (b - c) = nh + nk = n(h + k)$ de unde, $a \equiv c \pmod{n}$. S-a demonstrat astfel că relaţia de congruenţă modulo n este şi tranzitivă, deci o relaţie de echivalenţă.

Dacă $a \equiv a' \pmod{n}$ şi $b = b' \pmod{n}$, atunci $a - a' = nh$ şi $b - b' = nk$ cu $h, k \in \mathbb{Z}$. Cum $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = ank + nhb' = n(ak + hb')$, rezultă că $ab \equiv a'b' \pmod{n}$. La fel se arată că din $a \equiv a' \pmod{n}$ şi $b \equiv b' \pmod{n}$ rezultă $a + b \equiv a' + b' \pmod{n}$. Propoziţia este demonstrată.

Pentru $a \in \mathbb{Z}$ să notăm cu $a + n\mathbb{Z}$ mulţimea tuturor numerelor întregi de forma $a + nk$ cu $k \in \mathbb{Z}$. Cum relaţia de congruenţă modulo n este o relaţie de echivalenţă pe $\mathbb{Z}$, pentru $a \in \mathbb{Z}$ să notăm cu $\hat{a}$ clasa de echivalenţă a lui a faţă de această relaţie, numită *clasă de resturi modulo* n.

Propoziţia 1.2. *Pentru orice* $a \in \mathbb{Z}$ *avem* $\hat{a} = a + n\mathbb{Z}$.

Demonstraţie. Avem $x \in \hat{a} \Leftrightarrow x = a \pmod{n} \Leftrightarrow x - a = nk$ cu $k \in \mathbb{Z} \Leftrightarrow x \in a + n\mathbb{Z}$.

Propoziţia 1.3. *Numerele* $0, 1, 2, \ldots, n - 1$ *formează un sistem complet de reprezentanţi pentru relaţia de congruenţă modulo* n.

Demonstraţie. Conform definiţiei sistemului complet de reprezentanţi (vezi § 2, cap. I) trebuie arătat:

1) $i \not\equiv j \pmod{n}$ pentru $i, j \in \{0, 1, 2, \ldots, n - 1\}$, $i \neq j$.

2) Oricare ar fi $a \in \mathbb{Z}$, există $r \in \{0, 1, 2, \ldots, n - 1\}$ astfel încît $a \equiv r \pmod{n}$.

Dacă i şi j sînt ca la 1), atunci $0 < |i - j| < n$, de unde rezultă că n nu divide $i - j$, deci $i \not\equiv j \pmod{n}$. Dacă $a \in \mathbb{Z}$, atunci există $q, r \in \mathbb{Z}$ astfel încît

$$a = nq + r, \quad 0 \leqslant r < n,$$

Scanned with OKEN Scanner

(vezi teorema 3.6, cap. II), deci $a \equiv r \pmod{n}$ cu $r \in \{0, 1, 2, \ldots, n-1\}$ și 2) este de asemenea demonstrat.

Conform cu rezultatele asupra relațiilor de echivalență din § 2, cap. I, rezultă că pentru $a, b \in \mathbb{Z}$ avem

$$\hat{a} = \hat{b} \Leftrightarrow a \equiv b \pmod{n}.$$

Să notăm cu $\mathbb{Z}_n$ mulțimea claselor de echivalență a relației de echivalență studiată mai sus (congruența modulo n). Conform propoziției 1.3, $\mathbb{Z}_n$ este o mulțime cu n elemente, mai precis:

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{n-1}\}.$$

Pe mulțimea $\mathbb{Z}_n$ a claselor de resturi modulo n se introduc operațiile de adunare și înmulțire a claselor de resturi modulo n în modul următor:

$$\hat{a} + \hat{b} \overset{\text{def}}{=} \widehat{a+b},$$

respectiv

$$\hat{a}\hat{b} \overset{\text{def}}{=} \hat{ab},$$

oricare ar fi $\hat{a}, \hat{b} \in \mathbb{Z}_n$.

Așadar, dacă $U, V \in \mathbb{Z}_n$, atunci $U+V$ și UV se definesc astfel: se alege $a \in U$ și $b \in V$ (deci $U = \hat{a}$ și $V = \hat{b}$ conform propoziției 3.1, cap. I), se face suma $a+b$ și produsul ab în inelul $\mathbb{Z}$ și punem

$$U + V \overset{\text{def}}{=} \widehat{a+b},$$

respectiv

$$UV \overset{\text{def}}{=} \hat{ab}.$$

Scanned with OKEN Scanner

Dacă $a' \in U$ și $b' \in V$ (deci din nou $U = \hat{a}'$ și $V = \hat{b}'$), atunci $a \equiv a' \pmod{n}$ și $b \equiv b' \pmod{n}$. Conform propoziției 1.1 avem

$$\widehat{a+b} = \widehat{a'+b'}, \quad \hat{a}\hat{b} = \widehat{a'b'}.$$

Cu alte cuvinte, clasa *sumă* $U + V$ și clasa *produs* UV astfel definite nu depind de modul cum am ales reprezentanții a, b pentru U, respectiv V. Spunem că suma $U + V$ și produsul UV sînt bine definite, adică nu depind de reprezentanții acestor clase folosiți în construcția lui $U + V$ și UV.

Cînd $n = 6$, tablele adunării și înmulțirii claselor de resturi modulo 6 sînt:

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{5}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{0}$	$\hat{2}$	$\hat{4}$
$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$	$\hat{0}$	$\hat{3}$
$\hat{4}$	$\hat{0}$	$\hat{4}$	$\hat{2}$	$\hat{0}$	$\hat{4}$	$\hat{2}$
$\hat{5}$	$\hat{0}$	$\hat{5}$	$\hat{4}$	$\hat{3}$	$\hat{2}$	$\hat{1}$

Adunarea și înmulțirea claselor de resturi modulo n au proprietățile:

1° $(\hat{a} + \hat{b}) + \hat{c} = \hat{a} + (\hat{b} + \hat{c})$.

2° $\hat{a} + \hat{b} = \hat{b} + \hat{a}$.

3° $\hat{a} + \hat{0} = \hat{a}$.

4° $\hat{a} + \widehat{-a} = \hat{0}$.

5° $(\hat{a}\hat{b})\,\hat{c} = \hat{a}\,(\hat{b}\,\hat{c})$.

Scanned with OKEN Scanner

6° $\hat{a}\hat{b} = \hat{b}\hat{a}$.

7° $\hat{a} \cdot \hat{1} = \hat{a}$.

8° $\hat{a}(\hat{b} + \hat{c}) = \hat{a}\hat{b} + \hat{a}\hat{c}$.

Aşadar, adunarea claselor de resturi modulo n este asociativă, comutativă, admite pe $\hat{0}$ drept element de efect nul şi orice clasă $\hat{a}$ are opus faţă de operaţia de adunare a claselor, anume $-\hat{a} = \widehat{-a}$.

Înmulţirea claselor de resturi modulo n este asociativă, comutativă, admite pe $\hat{1}$ ca element de efect nul şi este distributivă faţă de operaţia de adunare a claselor de resturi modulo n.

Demonstraţia lor se dă pe baza proprietăţilor similare ale adunării şi înmulţirii inelului $\mathbb{Z}$ al numerelor întregi.

Astfel:

$$\hat{a} + \hat{b} = \widehat{a+b} = \widehat{b+a} = \hat{b}+\hat{a}$$

şi

$$\hat{a}(\hat{b} + \hat{c}) = \hat{a}\,\widehat{b + c} = \widehat{a(b+c)} = \widehat{ab+ac} =$$

$$= \widehat{ab} + \widehat{ac} = \hat{a}\hat{b} + \hat{a}\hat{c},$$

ceea ce reprezintă o demonstraţie pentru 2), respectiv 8).

Rezumînd cele de mai sus, rezultă:

Teorema 1.4. *Mulţimea* $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{n-1}\}$ *a claselor de resturi modulo n formează inel comutativ şi unitar faţă de operaţiile de adunare şi înmulţire a claselor de resturi.*

Un inel $\mathbb{Z}_n$ poate avea divizori ai lui zero. Astfel, în $\mathbb{Z}_6$ avem $\hat{2} \neq \hat{0}$, $\hat{3} \neq \hat{0}$ şi $\hat{2} \cdot \hat{3} = \hat{6} = \hat{0}$.

Lema 1.5. *O clasă de resturi* $\hat{a} \in \mathbb{Z}_n$ *este inversabilă în inelul* $\mathbb{Z}_n$ *dacă şi numai dacă* $(a, n) = 1$.

Scanned with OKEN Scanner

Demonstrație. Fie $\hat{a}$ un element inversabil al inelului $\mathbb{Z}_n$. Există $\hat{h} \in \mathbb{Z}_n$ astfel încît $\hat{a}\hat{h} = \hat{1}$. Deci $\widehat{ah} = \hat{1}$, de unde $ah - 1 = nk$ cu $k \in \mathbb{Z}$. Din egalitatea $ah + n(-k) = 1$ rezultă acum $(a, n) = 1$.

Reciproc, dacă $(a, n) = 1$, există $h, k \in \mathbb{Z}$ astfel încît $ah + nk = 1$ (vezi teorema 3.1, cap. III), Avem

$$\hat{1} = \widehat{ah + nk} = \hat{a}\hat{h} + \hat{n}\hat{k} = \hat{a}\hat{h} + \hat{0}\hat{k} = \hat{a}\hat{h},$$

deci $\hat{a}$ este element inversabil, $\hat{a}^{-1} = \hat{h}$.

Corolarul 1.6. *Inelul $\mathbb{Z}_n$ este corp dacă și numai dacă n este prim.*

Demonstrație. Presupunem că $\mathbb{Z}_n$ este corp. Dacă n nu este prim, atunci există $a, b \in \mathbb{Z}$ astfel încît

$$n = ab, \quad 1 < a < n, \quad 1 < b < n.$$

Avem $\hat{a} \neq \hat{0}$, $\hat{b} \neq \hat{0}$ și $\hat{a} \cdot \hat{b} = \widehat{ab} = \hat{n} = \hat{0}$. Înmulțind egalitatea $\hat{a} \cdot \hat{b} = \hat{0}$ cu inversul elementului $\hat{a}$, obținem $\hat{b} = \hat{0}$ (contradicție !). Deci n este prim.

Reciproc, dacă n este prim, atunci pentru orice $a \in \mathbb{Z}$, $1 \leqslant a < n$, avem $(a, n) = 1$. Din lema 1.5 rezultă că $\hat{a}$ este inversabil în $\mathbb{Z}_n$. Rezultă că orice clasă $\neq \hat{0}$ din $\mathbb{Z}_n$ este inversabilă în $\mathbb{Z}_n$, deci $\mathbb{Z}_n$ este corp.

Astfel $\mathbb{Z}_5 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$ este corp, 5 fiind număr prim.

Avem

$$\hat{1}^{-1} = \hat{1}, \quad \hat{2}^{-1} = \hat{3}, \quad \hat{3}^{-1} = \hat{2}, \quad \hat{4}^{-1} = \hat{4}.$$

O clasă $\hat{a} \in \mathbb{Z}_n$ este *clasă de resturi primă modulo n* dacă $(a, n) = 1$. Conform lemei 1.5 clasele de resturi prime modulo n sînt exact elemente inversabile ale inelului $\mathbb{Z}_n$, deci unitățile acestui inel. În particular, rezultă că mulțimea G_n a claselor de resturi prime modulo n formează grup față de operația de înmulțire a claselor, numit

Scanned with OKEN Scanner

grupul claselor de resturi prime modulo n. Acest lucru se putea stabili și direct observînd că din $(a, n) = 1$ și $(b, n) = 1$, rezultă $(ab, n) = 1$, deci dacă $\hat{a}$ și $\hat{b}$ sînt clase de resturi prime modulo n, la fel este $\hat{a}\hat{b}$. De asemenea, o clasă $\hat{a}$ de resturi primă modulo n este inversabilă (vezi lema 1.5) și dacă $\hat{b}$ este inversa lui $\hat{a}$, atunci $\hat{a}\hat{b} = 1$. Rezultă că $\hat{b}$ este de asemenea inversabilă, deci $(b, n) = 1$, de unde $\hat{b} \in G_n$.

Dacă $n = 9$, atunci numerele întregi a, $1 \leqslant a < 9$ astfel încît $(a, 9) = 1$ sînt 1, 2, 4, 5, 7, 8, deci $G_9 = \{\hat{1}, \hat{2}, \hat{4}, \hat{5}, \hat{7}, \hat{8}\}$.

§ 2. Elemente de ordin finit într-un grup

Fie G un grup. Vom folosi pentru operația grupului G notația multiplicativă și vom nota cu e elementul neutru al lui G. Evident, definițiile și rezultatele care urmează pot fi reformulate în notația aditivă. Amintim cîteva fapte expuse în cap. II, § 5.

O submulțime nevidă H a grupului G este *subgrup* al lui G dacă și numai dacă, oricare ar fi x, y din H, rezultă $xy^{-1} \in H$. Iată un alt exemplu de subgrup, care nu apare printre cele din paragraful menționat. Dacă G este grupul multiplicativ $\mathbb{C}^*$ al numerelor complexe nenule, iar

$$H = \{1, -1, i, -i\},$$

atunci H este un subgrup al lui G. Într-adevăr, tabla înmulțirii elementelor lui H

·	1	−1	i	−i
1	1	i	−i	−i
−1	−1	1	−i	i
i	i	−1	1	1
−i	−i	i	1	−1

arată că, oricare ar fi $x, y \in H$, $xy^{-1} \in H$.

Scanned with OKEN Scanner

Pentru orice grup G, submulțimile $E = \{e\}$ și G ale lui G sînt subgrupuri ale lui G; E se numește *subgrupul unitate* al lui G, iar în notația aditivă, subgrupul $0 = \{0\}$ se numește *subgrupul zero* al lui G.

Amintim, de asemenea, că dacă $n \in \mathbb{Z}$, $n \geqslant 0$, mulțimea $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ este subgrup al grupului aditiv $\mathbb{Z}$ al numerelor întregi și, mai mult, orice subgrup al grupului aditiv $\mathbb{Z}$ este de această formă.

Fie acum G din nou un grup dat în notație multiplicativă și $a \in G$. Pentru orice $n \in \mathbb{Z}$ definim:

$$a^n = \begin{cases} \underbrace{aa \ldots a}_{n}, & \text{dacă } n > 0, \\ e, & \text{dacă } n = 0, \\ \underbrace{a^{-1}a^{-1} \ldots a^{-1}}_{n}, & \text{dacă } n < 0. \end{cases}$$

Se verifică ușor prin inducție că

$$a^m a^n = a^{m+n} \text{ și } (a^m)^n = a^{mn},\ (a^n)^{-1} = a^{-n},$$

oricare ar fi $m, n \in \mathbb{Z}$.

Dacă grupul G este dat în notație aditivă, atunci definim:

$$na = \begin{cases} \underbrace{a + a \ldots + a}_{n}, & \text{dacă } n > 0, \\ 0, & \text{dacă } n = 0, \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{n}, & \text{dacă } n < 0. \end{cases}$$

și avem

$$ma + na = (m + n)a,\ m(na) = (mn)a, -(na) = (-n)a,$$

oricare ar fi $m, n \in \mathbb{Z}$.

Scanned with OKEN Scanner

Să notăm cu $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. Este clar că $\langle a \rangle$ este subgrup al lui G, numit *subgrupul ciclic generat de* a. Un grup G se numește *ciclic* dacă există $a \in G$ astfel încît $G = \langle a \rangle$.

Definiția 2.1. Se spune că un *element* a al grupului G este *de ordin finit*, dacă există $i, j \in \mathbb{Z}$, $i \neq j$, astfel încît $a^i = a^j$. În caz contrar se spune că a este *element de ordin infinit*.

Propoziția 2.1. *Un element* $a \in G$ *este de ordin finit dacă și numai dacă există* $k \in \mathbb{Z}$, $k > 0$, *astfel încît* $a^k = e$.

Demonstrație. Fie a un element de ordin finit și fie $i, j \in \mathbb{Z}$, $i \neq j$, astfel încît $a^i = a^j$. Dacă $i < j$, atunci

$$e = a^0 = a^{i+(-i)} = a^i a^{-i} = a^j a^{-i} = a^{j-i},$$

deci $a^k = e$, unde $k = j - i > 0$. Analog, se analizează cazul $i > j$.

Reciproc, dacă $a^k = e$, unde $k > 0$, atunci $a^k = e = a^0$ și $k \neq 0$. Propoziția este demonstrată.

Dacă $a \in G$ este element de ordin finit, atunci cel mai mic întreg strict pozitiv n astfel încît $a^n = e$ se numește *ordinul lui* a și se notează ord a. Deci :

$$\text{ord } a = \min \{k \mid a^k = e, \ k > 0\}.$$

Dacă $a \in G$ este element de ordin infinit, scriem ord $a = \infty$.

Propoziția 2.2. *Fie* a *un element de ordin finit al grupului* G *și* n *un întreg strict pozitiv. Atunci* $n = \text{ord } a$ *dacă și numai dacă sînt satisfăcute următoarele două condiții* :

1) $a^n = e$;

2) $a^k = e$, $k \in \mathbb{Z} \Rightarrow n \mid k$.

Demonstrație. Fie $n = \text{ord } a$. Atunci 1) rezultă din definiția numărului ord a. Fie $k \in \mathbb{Z}$ astfel încît $a^k = e$. Există $q, r \in \mathbb{Z}$ astfel încît $k = nq + r$, $0 \leqslant r < n$, și avem

$$a^r = a^{k-nq} = a^k (a^n)^{-q} = ee^{-q} = e.$$

Scanned with OKEN Scanner

Cum $0 \leqslant r < n$, din definiția lui n rezultă că $r = 0$, deci $n \mid k$.

Reciproc, dacă n satisface 1) și 2) iar $a^k = e$ cu $k > 0$, din 2) rezultă că $n \mid k$, deci $n \leqslant k$. Deci n este cel mai mic printre întregii $k > 0$ astfel încît $a^k = e$, de unde $n = \text{ord } a$.

Teorema 2.3. *Dacă $a \in G$ este element de ordin n, atunci subgrupul $\langle a \rangle$ are exact n elemente distincte și*

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Demonstrație. Fie $i, j \in \mathbb{Z}$, $0 \leqslant i, j < n$, astfel încît $a^i = a^j$. Atunci $a^{j-i} = e$ și $0 \leqslant |j - i| < n$. Cum $a^{j-i} = e$, rezultă că $n \mid j - i$. Din $0 \leqslant |j - i| < n$ rezultă $i = j$. Așadar, $a^i \neq a^j$ pentru $i \neq j$, $0 \leqslant i, j < n$, deci mulțimea $\{e, a, a^2, \ldots, a^{n-1}\}$ are n elemente. Pentru a termina demonstrația este suficient să dovedim că avem egalitatea din enunț. Cum $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$, este suficient să dovedim incluziunea contrară. Fie $x \in \langle a \rangle$. Atunci $x = a^k$, $k \in \mathbb{Z}$. Fie $q, r \in \mathbb{Z}$ astfel încît $k = nq + r$, $0 \leqslant r < n$. Avem

$$a^k = a^{nq+r} = (a^n)^q a^r = ea^r = a^r,$$

de unde $x \in \{e, a, a^2, \ldots, a^{n-1}\}$.

Propunem cititorului să arate:

1. Numărul complex i este element de ordinul al patrulea al grupului $(\mathbb{C}^*, \cdot)$ și $\langle i \rangle = \{1, -1, i, -i\}$.

2. Numărul complex

$$z = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

este element de ordin n al grupului $(\mathbb{C}^*, \cdot)$ și

$$\langle z \rangle = \left\{1, \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}, \ldots, \cos \frac{2(n-1)\pi}{n} + i \sin \frac{2(n-1)\pi}{n}\right\}.$$

3. Dacă $a \in G$, $\text{ord } a = n = st$, $s > 0$, $t > 0$ și $b = a^s$, atunci $\text{ord } b = t$.

Scanned with OKEN Scanner

4. Dacă $a, b \in G$, ord $a = m$, ord $b = n$, $ab = ba$ şi $(m, n) = 1$, atunci ord $ab = mn$.

5. Clasa $\hat{2}$ este element de ordinul al treilea al grupului G_7.

6. Dacă $z = a + ib$ este număr complex nenul şi $a^2 + b^2 \neq 1$, atunci este element de ordin infinit al grupului $(\mathbb{C}^*, \cdot)$.

§ 3. Teorema lui Lagrange. Consecinţe

Fie G un grup şi H un subgrup al său. Presupunem că G este dat în notaţie multiplicativă. Definiţiile şi rezultatele următoare pot fi reformulate cu uşurinţă şi în notaţie aditivă. Presupunem că G este comutativ, cu toate că problematica acestui paragraf poate fi abordată şi pentru grupuri necomutative.

Dacă $a, b \in G$, se spune că *a este congruent cu b modulo H* şi se scrie $a \equiv b \pmod{H}$, dacă şi numai dacă $ab^{-1} \in H$. Deci

$$a \equiv b \pmod{H} \Leftrightarrow ab^{-1} \in H.$$

Propoziţia 3.1. *Fie G un grup şi H un subgrup al lui G. Atunci relaţia de congruenţă modulo H este o relaţie de echivalenţă pe G. Pentru orice $a \in G$ avem*

$$\hat{a} = Ha = \{ha \mid h \in H\} = aH.$$

Demonstraţie. Pentru orice $x \in H$ avem $x \equiv x \pmod{H}$, fiindcă $xx^{-1} = e \in H$, deci relaţia de congruenţă modulo H este reflexivă. Dacă $x \equiv y \pmod{H}$, atunci $xy^{-1} \in H$, de unde $yx^{-1} = (xy^{-1})^{-1} \in H$, ceea ce implică $y \equiv x \pmod{H}$, adică această relaţie este şi simetrică. În sfîrşit, dacă $x \equiv y \pmod{H}$ şi $y \equiv z \pmod{H}$, atunci $xy^{-1} \in H$ şi $yz^{-1} \in H$. Rezultă că $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$, de unde $x \equiv z \pmod{H}$, deci relaţia este şi tranzitivă.

Avem $x \in \hat{a} \Leftrightarrow x \equiv a \pmod{H} \Leftrightarrow xa^{-1} = h$, cu $h \in H \Leftrightarrow$ $\Leftrightarrow x = ha = ah$ cu $h \in H$, de unde $\hat{a} = Ha = aH$ (grupul G este presupus comutativ).

Scanned with OKEN Scanner

Evident, dacă G este dat în notaţie aditivă, atunci

$$a \equiv b(\text{mod } H) \Leftrightarrow a - b \in H$$

şi avem

$$\widehat{a} = H + a = \{h + a \mid h \in H\} = a + H.$$

Observaţie. Dacă G este grupul aditiv $\mathbb{Z}$ al numerelor întregi şi H un subgrup $\neq 0$ al acestuia, există $n > 0$ astfel încît $H = {}^{n}\mathbb{Z}$. Este clar că pentru $a, b \in \mathbb{Z}$ avem

$$a \equiv b(\text{mod } H) \Leftrightarrow a \equiv b(\text{mod } n)$$

iar

$$\widehat{a} = n\mathbb{Z} + a = \{nk + a \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Fie G un grup finit (grup cu un număr finit de elemente). Notăm cu ord G numărul elementelor grupului G, numit *ordinul lui* G. Dacă H este subgrup al lui G, vom nota cu ord H numărul elementelor lui H, numit *ordinul subgrupului* H. Prin indicele lui H în G, notat cu $[G : H]$, se înţelege numărul claselor de echivalenţă a relaţiei de congruenţă modulo H.

Să observăm că aplicaţia

$$f : H \to Ha,\ f(h) = ha,\ h \in H,$$

este bijectivă. Într-adevăr, dacă $f(h_1) = f(h_2)$, atunci $h_1 a = h_2 a$, de unde

$$h_1 = (h_1 a)a^{-1} = (h_2 a)a^{-1} = h_2$$

şi deci f este injectivă. Dacă $y \in Ha$, $y = ha$ cu $h \in H$, atunci $f(h) = ha = y$, de unde rezultă că f este aplicaţie surjectivă. Deci orice clasă de echivalenţă Ha are acelaşi număr de elemente ca şi H. Întrucît G este grup finit, orice sistem complet de reprezentanţi al relaţiei de congruenţă modulo H este finit. Fie $a_1, a_2, \ldots, a_r$ un asemenea sistem. Este clar că $r = [G : H]$. Conform rezultatelor din § 2, cap. I, avem

Scanned with OKEN Scanner

$$G = \bigcup_{i=1}^{r} Ha_i,\ Ha_i \cap Ha_j = \emptyset \text{ pentru } i \neq j.$$

Rezultă că ord $G = [G : H]$ ord H şi deci am demonstrat :

Teorema 3.2 (*Lagrange*). *Dacă G este un grup finit şi H un subgrup al său, atunci* ord H *şi* $[G : H]$ *sînt divizori ai lui* ord G. *Mai precis* :

$$\text{ord } G = [G : H] \text{ ord } H.$$

Sîntem acum în măsură să demonstrăm un rezultat foarte util pentru cele ce urmează.

Corolarul 3.3. *Dacă G este grup finit, atunci toate elementele sale sînt de ordin finit şi*

$$\text{ord } a \mid \text{ord } G, \textit{ oricare ar fi } a \in G.$$

Demonstraţie. Cum G este finit, elementele a^k, $k \in \mathbb{Z}$ nu pot fi distincte două cîte două. Deci există $i, j \in \mathbb{Z}$, $i \neq j$, astfel încît $a^i = a^j$, de unde rezultă că a este element de ordin finit. Fie $H = \langle a \rangle$. Conform teoremei 2.3, avem ord $a =$ $=$ ord H şi din teorema lui Lagrange rezultă că ord $a \mid$ ord G.

Fie n un număr natural nenul. Să notăm cu $\varphi(n)$ numărul întregilor a astfel încît

$$(a, n) = 1,\ 1 \leqslant a < n.$$

Numărul $\varphi(n)$ se numeşte *indicatorul lui Euler* al numărului n.

Dacă p este număr prim, atunci $(a, p) = 1$ pentru orice a, $1 \leqslant a < p$, de unde

$$\varphi(p) = p - 1.$$

Dacă $n = p^e$, cu p prim şi e întreg $\geqslant 1$, atunci numerele a, $1 \leqslant a < n$, astfel încît $(a, n) \neq 1$ sînt

$$0, p, 2p, 3p, \ldots, p^2, 2p^2, 3p^2, \ldots, (p-1)p^{e-1},$$

Scanned with OKEN Scanner

de unde rezultă

$$\varphi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right).$$

Cum $0, 1, 2, \ldots, n-1$ formează un sistem complet de reprezentanți pentru relația de congruență modulo n (vezi propoziția 1.3), deducem că elementele grupului G_n pot fi descrise astfel:

$$G_n = \{\hat{a} \mid 1 \leqslant a < n,\ (a, n) = 1\},$$

de unde obținem:

Propoziția 3.4. *Pentru orice $n > 0$, ordinul grupului G_n al claselor de resturi prime modulo n este egal cu $\varphi(n)$.*

Iată acum o aplicație importantă a teoremei lui Lagrange.

Teorema 3.5 (*Euler*). *Dacă n este un număr diferit de zero și $a \in \mathbb{Z}$, $(a, n) = 1$, atunci*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Demonstrație. Din $(a, n) = 1$, rezultă că $\widehat{a_n} \in G_n$. Cum G_n este grup finit de ordin $\varphi(n)$, există $m \in \mathbb{N}$ astfel încît

$$\varphi(n) = m \cdot \operatorname{ord} \widehat{a}$$

(vezi corolarul 3.3), de unde

$$\widehat{a^{\varphi(n)}} = \hat{a}^{\varphi(n)} = (\hat{a}^{\operatorname{ord}\,\hat{a}})^m = \hat{1}^m = \hat{1}.$$

Din $\widehat{a^{\varphi(n)}} = \hat{1}$ deducem că $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corolar 3.6 (*Fermat*). *Fie $a \in \mathbb{Z}$ și p un număr prim > 0 astfel încît p nu divide pe a. Atunci*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Scanned with OKEN Scanner

Demonstrație. Cum p nu divide pe a, avem $(a, p) = 1$. Pe de altă parte $\varphi(p) = p - 1$ și acum teorema lui Fermat rezultă din teorema lui Euler.

§ 4. Congruențe

Fie m un număr natural > 1 și

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

un polinom cu coeficienți întregi. Ne propunem să găsim numerele întregi x astfel încît $m \mid f(x)$, ceea ce înseamnă, cu o terminologie consacrată, a rezolva congruența

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \equiv 0 \pmod{m}. \quad (5.1)$$

Dacă în (5.1) a_n nu se divide prin m, spunem că avem o *congruență de grad n.*

Dacă p este un număr prim, atunci teorema lui Fermat stabilește că soluțiile congruenței

$$X^{p-1} - 1 \equiv 0 \pmod{p}$$

sînt numerele întregi x care nu se divid prin p.

Congruența de gradul întîi

$$6X - 7 \equiv 0 \pmod{8}$$

nu are soluții. Într-adevăr, dacă $x \in \mathbb{Z}$ este o soluție a acestei congruențe, atunci există $k \in \mathbb{Z}$ astfel încît

$$6x - 7 = 8k,$$

ceea ce implică $2 \mid 7$ (contradicție!).

Să asociem polinomului $f = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ următorul polinom în X cu coeficienți în inelul de clase de resturi $\mathbb{Z}_m$:

Scanned with OKEN Scanner

$$\hat{f} = \hat{a}_n X^n + \ldots + \hat{a}_1 X + \hat{a}_0 \in \mathbb{Z}_m[X],$$

numit *redusul modulo m al lui f*. Să observăm că

$$\deg \hat{f} = n \Leftrightarrow \hat{a}_n \neq 0 \Leftrightarrow a_n \not\equiv 0 (\text{mod } m).$$

Propoziția 4.1. *Un număr întreg x este soluție a congruenței*

$$a_n X^n + \ldots + a_1 X + a_0 \equiv 0 \ (\text{mod } m)$$

dacă și numai dacă $\hat{x} \in \mathbb{Z}_n$ *este rădăcină a ecuației*

$$\hat{a}_n X^n + \ldots + \hat{a}_1 X + \hat{a}_0 = \hat{0}.$$

Cu alte cuvinte, $m | f(x)$ *dacă și numai dacă* $\hat{f}(\hat{x}) = \hat{0}$, *unde* $f = a_n X^n + \ldots + a_1 X + a_0$.

Demonstrație. Dacă $x \in \mathbb{Z}$ este astfel încît

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (\text{mod } m),$$

atunci

$$\hat{0} = \overline{a_n x^n + \ldots + a_1 x + a_0} = \hat{a}_n \hat{x}^n + \ldots + \hat{a}_1 \hat{x} + \hat{a}_0 = \hat{f}(\hat{x}).$$

Reciproc, dacă $\hat{f}(\hat{x}) = \hat{0}$, atunci

$$\overline{a_n x^n + \ldots + a_1 x + a_0} = \hat{a}\,\hat{x}^n + \ldots + \hat{a}_1 \hat{x} + \hat{a}_0 = \hat{f}(\hat{x}) = \hat{0},$$

de unde

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (\text{mod } m).$$

Corolarul 4.2. *Dacă* $x \in \mathbb{Z}$ *este soluție a congruenței* (5.1) *și* $y \in \mathbb{Z}$ *este astfel încît* $y \equiv x (\text{mod } m)$, *atunci y este soluție a congruenței* (5.1).

Scanned with OKEN Scanner

Demonstrație. Cum x este soluție a congruenței (5.1), avem $\hat{f}(\hat{x}) = 0$. Din $y \equiv x \pmod{m}$ avem $\hat{y} = \hat{x}$, deci $\hat{f}(\hat{y}) = \hat{0}$ și din propoziția 4.1 rezultă că y este soluție a congruenței (5.1).

Observație. Inelul $\mathbb{Z}_m$ fiind finit, propoziția 4.1 și corolarul 4.2 ne dau o metodă enumerativă de a găsi soluțiile congruenței (5.1). Într-adevăr, este suficient să calculăm

$$\hat{f}(\hat{0}),\ \hat{f}(\hat{1}),\ \hat{f}(\hat{2}),\ \ldots,\ \hat{f}(\widehat{m-1})$$

și atunci soluțiile congruenței (5.1) sînt

$$\bigcup_{\hat{f}(\hat{r}) = \hat{0}, 0 \leqslant r < m} r + m\mathbb{Z}.$$

Astfel, soluțiile congruenței

$$X^2 + 4X - 3 \equiv 0 \pmod{6} \tag{5.2}$$

sînt numerele întregi

$$3 + 6\mathbb{Z} \cup 5 + 6\mathbb{Z},$$

deci numerele de forma $3 + 6k$ și $5 + 6k$, $k \in \mathbb{Z}$.

Într-adevăr, notînd cu $f = X^2 + 4X - 3$, avem

$$\hat{f}(\hat{0}) \neq \hat{0},\ \hat{f}(\hat{1}) \neq \hat{0},\ \hat{f}(\hat{2}) \neq \hat{0},\ \hat{f}(\hat{3}) = \hat{0},\ \hat{f}(\hat{4}) \neq \hat{0},\ \hat{f}(\hat{5}) = \hat{0}.$$

Congruența

$$X^2 + 3 = 0 \pmod{5}$$

nu are soluții, deoarece, notînd cu $f = X^2 + 3$, avem

$$\hat{f}(\hat{0}) \neq \hat{0},\ \hat{f}(\hat{1}) \neq \hat{0},\ \hat{f}(\hat{2}) \neq \hat{0},\ \hat{f}(\hat{3}) \neq \hat{0},\ \hat{f}(\hat{4}) \neq \hat{0}.$$

Definiția 4.1. Soluțiile $x_1, x_2, \ldots, x_n$ ale congruenței

$$a_n X^n + \ldots + a_1 X + a_0 \equiv 0 \pmod{m}$$

Scanned with OKEN Scanner

sînt *distincte modulo* m dacă $x_i \not\equiv x_j \pmod{m}$ pentru $i \neq j$.

Este clar că numărul maxim de soluţii distincte modulo m coincide cu numărul rădăcinilor distincte din $\mathbb{Z}_m$ al redusului modulo m al polinomului f. Evident, pentru a cunoaşte toate soluţiile congruenţei (5.1) este suficient să cunoaştem un sistem maximal $x_1, x_2, \ldots, x_r$ de soluţii distincte modulo m, căci atunci soluţiile congruenţei vor fi

$$\bigcup_{i=1}^{r} x_i + m\mathbb{Z}$$

(vezi corolarul 4.2).

Astfel, 3 şi 5 formează un sistem maximal de soluţii distincte modulo 6 pentru congruenţa (5.2).

Evident, numărul soluţiilor distincte modulo m este $\leqslant m$. Dacă modulul m este prim, atunci numărul soluţiilor distincte modulo m este mărginit şi de gradul congruenţei după cum rezultă din teorema următoare :

Teorema 4.3 (*Lagrange*). *Fie p un număr prim şi*

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \equiv 0 \pmod{p}$$

o congruenţă de grad n modulo p (deci $a_n \bmod p \neq 0$). Atunci numărul soluţiilor distincte modulo p ale acestei congruenţe nu depăşeşte n.

Demonstraţie. Demonstrăm teorema prin inducţie asupra lui n. Fie $n = 1$. Dacă x şi $x' \in \mathbb{Z}$ sînt soluţii ale congruenţei

$$a_1 X + a_0 \equiv 0 \pmod{p}, \tag{5.3}$$

atunci $a_1 x + a_0 \equiv 0 \pmod{p}$ şi $a_1 x' + a_0 \equiv 0 \pmod{p}$, de unde $a_1(x - x') \equiv 0 \pmod{p}$. Deci $p \mid a_1(x - x')$ şi cum p nu divide a_1 (prin ipoteză $a_1 \bmod p \not\equiv 0$), rezultă că $p \mid x - x'$,

de unde $x \equiv x' \pmod p$. Rezultă că numărul soluţiilor distincte modulo p ale congruenţei (5.3) este cel mult 1, deci teorema este demonstrată pentru $n = 1$.

Presupunem că $n > 1$ şi că teorema este adevărată pentru congruenţe de grad $n-1$. Să notăm cu f polinomul $a_n X^n + \ldots + a_1 X + a_0$. Fie $x_1, \ldots, x_r$ un sistem de soluţii distincte modulo p ale congruenţei

$$f(X) \equiv 0 \pmod p.$$

Trebuie să arătăm că $r \leqslant n$. Împărţind pe f prin $X - x_1$, obţinem

$$f = (X - x_1)\, g + r$$

cu $g \in \mathbb{Z}[X]$, $\deg(g) = n - 1$ şi $r \in \mathbb{Z}$. Întrucît $f(x_1) = r$ şi $f(x_1) \equiv 0 \pmod p$, rezultă că $p \mid r$. Avem $(x_i - x_1)g(x_i) + r = f(x_i) \equiv 0 \pmod p$, $2 \leqslant i \leqslant r$, deci $p \mid (x_i - x_1)g(x_i)$, $2 \leqslant i \leqslant r$. Deoarece p nu divide pe $x_i - x_1$, $2 \leqslant i \leqslant r$ ($x_1, \ldots, x_r$ fiind soluţii distincte modulo p), rezultă că $p \mid g(x_i)$, $2 \leqslant i \leqslant r$, deci

$$g(x_i) \equiv 0 \pmod p, \quad 2 \leqslant i \leqslant r.$$

Este clar că $g = a_n X^{n-1} + \ldots$ şi cum $a_n \pmod p \neq 0$, rezultă că congruenţa

$$g(X) \equiv 0 \pmod p$$

are gradul $n - 1$ şi $x_2, \ldots, x_r$ sînt soluţii ale acesteia, distincte modulo p. Conform ipotezei inducţiei, avem $r - 1 \leqslant n - 1$, deci $r \leqslant n$.

Observaţie. Pentru cititorul familiarizat cu teoria corpurilor dăm următoarea demonstraţie imediată a teoremei 4.3: $\mathbb{Z}_p$ fiind corp, polinomul $\hat{f} \in \mathbb{Z}_p[X]$, $\deg(\hat{f}) = n$, are cel mult n rădăcini distincte şi deci cel mult n rădăcini distincte în $\mathbb{Z}_p$. Se aplică apoi propoziţia 4.1.

Corolarul 4.4. *Dacă congruenţele de grad n*

$$aX^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \equiv 0 \pmod p,$$

$$aX^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0 \equiv 0 \pmod p,$$

unde p este prim, admit în comun n rădăcini distincte modulo p, atunci $a_i \equiv b_i \pmod p$, $0 \leqslant i < n$.

Demonstrație. Dacă există $k \in \mathbb{N}$, $0 \leqslant k < n$, astfel încît $a_k \not\equiv b_k \pmod p$, atunci congruența

$$(a_l - b_l)X^l + \ldots + (a_1 - b_1)X + a_0 - b_0 \equiv 0 \pmod p,$$

unde

$$l = \max \{k \mid a_k \not\equiv b_k \pmod p\}$$

are gradul $l < n$ și admite n rădăcini distincte modulo p, deci se obține o contradicție (vezi teorema 4.3). Rămîne adevărat că $a_i \equiv b_i \pmod p$, $0 \leqslant i < n$.

Corolarul 4.5 (*Wilson*). *Dacă p este un număr prim, atunci*

$$(p - 1)! + 1 \equiv 0 \pmod p.$$

Demonstrație. Pentru $p = 2$ afirmația din enunț se verifică direct. Dacă $p \neq 2$, atunci p este impar. Teorema lui Fermat arată că $1, 2, \ldots, p - 1$ sînt soluții (distincte modulo p) ale congruenței

$$X^{p-1} - 1 \equiv 0 \pmod p.$$

Aceleași soluții admite și congruența de grad $p - 1$:

$$(X - 1)(X - 2) \ldots (X(p - 1)) \equiv 0 \pmod p.$$

Cum $p - 1$ este par, termenul liber al polinomului $(X - 1)(X - 2) \ldots (X - (p - 1))$ este

$$(-1)(-2) \ldots (-(p - 1)) = (-1)^{p-1}(p - 1)! =$$

$$= (p - 1)!.$$

Aplicînd corolarul 4.4, deducem că $(p - 1)! \equiv -1 \pmod p$.

Scanned with OKEN Scanner

Vom întreprinde în continuare studiul congruenţelor de gradul întîi faţă de un modul $m > 1$, nu obligatoriu număr prim. O asemenea congruenţă poate fi pusă sub forma

$$aX \equiv b \pmod{m}, \quad a \bmod m \neq 0.$$

Teorema 4.6. *O congruenţă de gradul întîi modulo m*

$$aX \equiv b \pmod{m}, \; a \bmod m \neq 0, \tag{5.4}$$

admite soluţii dacă şi numai dacă $d \mid b$, unde $d = (a, m)$. În acest caz numărul soluţiilor distincte modulo m este egal cu d.

Demonstraţie. Fie $x \in \mathbb{Z}$ o soluţie a congruenţei (5.4). Atunci există $k \in \mathbb{Z}$ astfel încît $ax = b + km$, de unde $d \mid b$.

Reciproc, dacă $d \mid b$, fie $a_1, b_1, m_1 \in \mathbb{Z}$, astfel încît $a = da_1$, $b = db_1$, $m = dm_1$. Este clar că pentru orice $x \in \mathbb{Z}$ avem

$$m \mid ax - b \Leftrightarrow m_1 \mid a_1 x - b_1,$$

de unde rezultă că congruenţa (5.4) are aceleaşi soluţii ca şi congruenţa următoare:

$$a_1 X \equiv b_1 \pmod{m_1}. \tag{5.5}$$

Întrucît $a \bmod m \neq 0$, rezultă că $a_1 \bmod m_1 \neq 0$, deci congruenţa (5.5) are, de asemenea, gradul întîi. Avem

$$d = (a, m) = (da_1, dm_1) = d(a_1, m_1),$$

de unde $(a_1, m_1) = 1$. Fie $h, k \in \mathbb{Z}$ astfel încît $a_1 h + m_1 k = 1$. Rezultă

$$a_1 h b_1 + m_1 k k_1 = b_1,$$

deci

$$a_1 x \equiv b_1 \pmod{m_1},$$

Scanned with OKEN Scanner

unde $x = hb_1$. Aşadar, dacă $d|b$, congruenţa (5.5) admite o soluţie şi atunci, aşa cum s-a mai observat, congruenţa (5.4) admite soluţie. Prima parte a teoremei este astfel demonstrată.

Fie x_0 soluţie a congruenţei (5.5). Dacă $x \in \mathbb{Z}$ este o soluţie arbitrară a aceleiaşi congruenţe, atunci avem $a_1x_0 \equiv b_1 \pmod{m_1}$, $a_1x \equiv b_1 \pmod{m_1}$, de unde $a_1(x - x_0) \equiv 0 \pmod{m_1}$. Deci $m_1 | a_1(x - x_0)$ şi cum $(m_1, a_1) = 1$, rezultă $m_1 | x - x_0$, deci $x \equiv x_0 \pmod{m_1}$. Aşadar, soluţiile congruenţei (5.5) sînt

$$x = x_0 + m_1k, \quad k \in \mathbb{Z}. \tag{5.6}$$

Conform observaţiei de la începutul demonstraţiei, congruenţa (5.4) are ca soluţii exact numerele de la (5.6). Rămîne să arătăm că printre ele se găsesc exact d soluţii distincte modulo d. Vom arăta că soluţiile

$$x_0, x_0 + m_1, x_0 + 2m_1, \ldots, x_0 + (d - 1)m_1$$

sînt distincte modulo m şi că orice soluţie a congruenţei (5.4) este congruentă modulo m cu una dintre acestea. Astfel, demonstraţia teoremei se va încheia.

Fie $x = x_0 + im_1$, $y = x_0 + jm_1$, $0 \leqslant i, j < d$, $i \neq j$. Atunci

$$|x - y| = |(i - j)m_1| < dm_1 = m,$$

de unde rezultă că $x \not\equiv y \pmod{m}$, întrucît m nu poate divide $x - y$.

Fie x o soluţie arbitrară a congruenţei (5.4). Atunci x este un număr de la (5.6), deci $x = x_0 + m_1 k$, $k \in \mathbb{Z}$. Fie $q_1, r \in \mathbb{Z}$ astfel încît

$$k = dq + r, \quad 0 \leqslant r < d.$$

Avem

$$x = x_0 + (dq + r)m_1 = x_0 + mq + rm_1 \equiv x_0 + rm_1 \pmod{m}.$$

Scanned with OKEN Scanner

Observaţii. 1. O soluţie particulară a congruenţei de gradul întîi

$$a_1X \equiv b_1 (\text{mod } m_1),\ (a_1,\ m_1) = 1,$$

se poate afla, de asemenea, folosind teorema lui Euler. Într-adevăr, din $(a_1,\ m_1) = 1$ rezultă că $a_1^{\varphi(m_1)} \equiv 1 (\text{mod } m_1)$, de unde

$$a_1(a_1^{\varphi(m_1)-1}b_1) \equiv b_1 (\text{mod } m_1).$$

Aşadar, $x_0 = a_1^{\varphi(m_1)-1}b_1$ este o soluţie particulară a congruenţei (5.5). Totuşi, este de preferat soluţia particulară indicată în cursul demonstraţiei teoremei 4.6. Într-adevăr, determinarea întregilor h şi k astfel încît $a_1h + m_1k = 1$ (şi deci a soluţiei particulare $x_0 = hb_1$) se poate face cu un volum relativ mic de calcule folosind algoritmul lui Euclid extins (vezi § 5, cap. III). În schimb, calculul soluţiei particulare

$$x_0 = a_1^{\varphi(m_1)-1}b_1$$

presupune găsirea în prealabil a descompunerii în factori primi a lui m_1 (vezi § 5) şi apoi calculul puterii $a_1^{\varphi(m_1)-1}$, ceea ce, pentru a_1 şi m_1 numere mari, este un lucru anevoios.

2. Să considerăm ecuaţia

$$aX + mY = b \tag{5.7}$$

unde $a,\ b,\ m \in \mathbb{Z},\ m>0$. Se pune problema găsirii numerelor întregi x, y astfel încît $ax + my = b$. Cu alte cuvinte, ne propunem să rezolvăm o ecuaţie diofantică de gradul întîi cu două necunoscute. Este clar că există $x,\ y \in \mathbb{Z}$ astfel încît $ax + my = b$ dacă şi numai dacă $ax \equiv b (\text{mod } m)$. Cu alte cuvinte, ecuaţia diofantică (5.7) are soluţii dacă şi numai dacă congruenţa (5.4) are soluţii. Conform teoremei 4.6, ecuaţia diofantică (5.7) admite soluţii dacă şi numai dacă $d \mid b$, unde $d = (a,\ m)$. Notînd cu $a_1,\ b_1,\ m_1$ cîturile prin d ale lui $a,\ b,\ m$ respectiv, observăm că $x, y \in \mathbb{Z}$ este soluţie a ecuaţiei diofantice (5.7) dacă şi numai dacă este soluţie a ecuaţiei diofantice

$$a_1X + m_1Y = b_1, \quad (a_1,\ m_1) = 1. \tag{5.8}$$

Deci este suficient să găsim soluţiile ecuaţiei diofantice (5.8). O soluţie particulară $x_0,\ y_0$ se poate afla folosind algoritmul lui Euclid extins: determinăm $h,\ k \in \mathbb{Z}$ astfel încît $a_1h + m_1k = 1$ şi atunci $x_0 = hb_1,\ y_0 = kb_1$ este o soluţie particulară a ecuaţiei diofantice (5.8). O altă cale este să luăm

$$x_0 = a_1^{\varphi(m_1)-1}b_1,\ y_0 = \frac{a_1x_0 - b_1}{m_1}.$$

Scanned with OKEN Scanner

Fie acum $x, y \in \mathbb{Z}$ o soluție arbitrară a ecuației diofantice (5.8). Din $a_1x_0 + m_1y_0 = b_1$ și $a_1x + m_1y = b_1$ deducem

$$a_1(x - x_0) = m_1(y_0 - y).$$

Așadar, $m_1 \mid a_1(x - x_0)$ și cum $(a_1, m_1) = 1$, rezultă că $m_1 \mid x - x_0$. Fie $k \in \mathbb{Z}$ astfel încît $x - x_0 = km_1$, adică $x = x_0 + km_1$. Acum deducem că $y = y_0 - ka_1$. Rezultă că soluțiile ecuației diofantice (5.7) sînt

$$x = x_0 + km_1, \quad y = y_0 - ka_1, \qquad k \in \mathbb{Z}.$$

§ 5. Lema chinezească a resturilor

Ideea fundamentală a aritmeticii modulare este studiul unor probleme referitoare la numere întregi cu ajutorul resturilor acestora în raport cu unul sau mai multe numere naturale, $m_1, m_2, \ldots, m_r > 1$ numite module. În paragrafele precedente am studiat unele probleme de divizibilitate în acest spirit.

Un rezultat central în aritmetica modulară este lema chinezească a resturilor care raportează numerele întregi la un sistem finit de numere naturale $m_1, m_2, \ldots, m_r > 1$ astfel încît

$$(m_i, m_j) = 1 \quad \text{pentru } i \neq j.$$

Lema 5.1. *Fie $m_1, m_2, \ldots, m_r \in \mathbb{Z}$ astfel încît $(m_i, m_j) = 1$ pentru $i \neq j$. Pentru $a \in \mathbb{Z}$ avem:*

1) $(m_i, a) = 1, 1 \leqslant i \leqslant r \Rightarrow (m_1m_2 \ldots m_r, a) = 1$;

2) $m_i \mid a, 1 \leqslant i \leqslant r \Rightarrow m_1m_2 \ldots m_r \mid a$.

Demonstrație. 1) Fie $d = (m_1m_2 \ldots m_r, a)$. Dacă $d \neq 1$, atunci există $p \in \mathbb{Z}$ prim astfel încît $p \mid d$. Din $p \mid d$ și $d \mid m_1m_2 \ldots m_r$, rezultă că $p \mid m_1m_2 \ldots m_r$. Cum p este prim, există i astfel încît $p \mid m_i$. Dar avem și $p \mid a$, deci p divide pe $(m_i, a) = 1$ (contradicție !).

2) Afirmația este adevărată pentru $r = 1$. Fie $r > 1$ și facem ipoteza că 2) este adevărată pentru $r - 1$. Cum $(m_i, m_r) = 1, 1 \leqslant i \leqslant r - 1$, din 1) rezultă că

Scanned with OKEN Scanner

$$(m_1 m_2 \ldots m_{r-1}, m_r) = 1.$$

Fie $h, k \in \mathbb{Z}$ astfel încît

$$m_1 m_2 \ldots m_{r-1} h + m_r k = 1.$$

Conform ipotezei inducţiei, $m_1 m_2 \ldots m_{r-1} | a$. Dar

$$a = m_1 m_2 \ldots m_{r-1} ha + m_r ka$$

şi cum avem încă $m_r | a$, rezultă că $m_1 m_2 \ldots m_r$ divide fiecare termen din membrul al doilea al ultimei egalităţi şi atunci $m_1 m_2 \ldots m_r$ divide şi membrul întîi, deci pe a.

Teorema 5.2 (*lema chinezească a resturilor*). *Fie* $m_1, \ldots, m_r$ *numere naturale* >1 *astfel încît* $(m_i, m_j) = 1$ *pentru* $i \neq j$. *Atunci, oricare ar fi* $u, a_1, a_2, \ldots, a_n \in \mathbb{Z}$, *există* $a \in \mathbb{Z}$ *unic determinat astfel încît*

$$a \equiv a_i \pmod{m_i}, \quad 1 \leqslant i \leqslant r,$$

şi

$$u \leqslant a < a + m,$$

unde $m = m_1 m_2 \ldots m_r$.

Demonstraţie. Fie $a, a' \in \mathbb{Z}$ astfel încît $u \leqslant a < u + m$, $u \leqslant a' < u + m$, $a \equiv a_i \pmod{m_i}$, $a' \equiv a_i \pmod{m_i}$, $1 \leqslant i \leqslant r$. Atunci $|a - a'| < m$ şi $a \equiv a' \pmod{m_i}$, $1 \leqslant i \leqslant r$. Deci $m_i | a - a'$ pentru $i = 1, 2, \ldots, r$ şi din lema 5.1 rezultă că $m | a - a'$. Dar $|a - a'| < m$ şi $m | a - a'$ implică $a = a'$. Am demonstrat astfel partea de unicitate din enunţul lemei.

Să notăm cu F mulţimea tuturor sistemelor ordonate de r numere naturale

$$(d_1, d_2, \ldots, d_r), \quad 0 \leqslant d_i < m_i, \; 1 \leqslant i \leqslant r.$$

Scanned with OKEN Scanner

Este clar că F are m elemente. Tot din m elemente constă mulțimea E a numerelor naturale a astfel încît $u \leqslant a < u+m$. Reamintim că am convenit să notăm cu $a \bmod m_i$ restul împărțirii prin m_i a numărului întreg a, deci

$$0 \leqslant a \bmod m_i < m_i,\ 1 \leqslant i \leqslant r.$$

Fie funcția $\rho : E \to F$

$$\rho(a) = (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_r),$$

oricare ar fi $a \in E$. Conform primei părți a demonstrației, funcția ρ este injectivă. Din

$$\operatorname{card} E = \operatorname{card} F = m$$

rezultă că ρ este surjectivă, deci ρ este o bijecție.

Fie $d_i = a_i \bmod m_i$, $1 \leqslant i \leqslant r$. Cum ρ este aplicație surjectivă, există $a \in E$ astfel încît

$$a \bmod m_i = d_i, 1 \leqslant i \leqslant r.$$

Așadar,

$$a \bmod m_i = a_i \bmod m_i,\ 1 \leqslant i \leqslant r,$$

deci a și a_i au același rest prin împărțirea prin m_i, $1 \leqslant i \leqslant r$, de unde

$$a \equiv a_i \pmod{m_i}.$$

Corolarul 5.3. *Dacă $m_1, \ldots, m_r$ sînt numere naturale >1 astfel încît $(m_i, m_j) = 1$ pentru $i \neq j$, atunci sistemul de congruențe*

$$\begin{aligned} X &= a_1 \equiv 0 \pmod{m_1}, \\ X &- a_2 \equiv 0 \pmod{m_2}, \\ &\cdots\cdots\cdots \\ X &- a_r \equiv 0 \pmod{m_r} \end{aligned}$$

Scanned with OKEN Scanner

admite o soluție $a \in \mathbb{Z}$ *și numai una, astfel încît* $u \leqslant a < u + m$, *oricare ar fi* $u \in \mathbb{Z}$, *unde* $m = m_1 m_2 \ldots m_r$.

Observație. Demonstrația părții de existență din lema chineză a resturilor este neconstructivistă. Iată o demonstrație care oferă și o metodă de calcul al numărului $a \in \mathbb{Z}$ astfel încît $a \equiv a_i \pmod{m_i}$, $1 \leqslant i \leqslant r$. Fie

$$q_i = \frac{m}{m_i} = m_1 \ldots m_{i-1} m_{i+1} \ldots m_r, \qquad 1 \leqslant i \leqslant r,$$

și

$$e_i = q_i^{\varphi(m_i)}, \quad 1 \leqslant i \leqslant r.$$

Deoarece $(m_i, m_j) = 1$ pentru $i \neq j$, rezultă că

$$(m_i, q_i) = 1, \qquad 1 \leqslant i \leqslant r$$

[vezi lema 5.1, 1)]. Aplicînd teorema lui Euler, obținem

$$q_i^{\varphi(m_i)} \equiv 1 \pmod{m_i}, \qquad 1 \leqslant i \leqslant r.$$

Cum $q_i \equiv 0 \pmod{m_j}$ pentru $i \neq j$, avem încă

$$q_i^{\varphi(m_i)} \equiv 0 \pmod{m_j}, \quad i \neq j.$$

Așadar, $e_i \equiv 1 \pmod{m_i}$, $1 \leqslant i \leqslant r$, și $e_i \equiv 0 \pmod{m_j}$ pentru $i \neq j$.

Fie $b = a_1 e_1 + a_2 e_2 + \ldots + a_r e_r$. Avem

$$b - a_i = a_i (e_i - 1) + \sum_{j \neq i} a_j e_j \equiv 0 \pmod{m_i}, \quad 1 \leqslant i \leqslant r,$$

de unde

$$b \equiv a_i \pmod{m_i} \qquad 1 \leqslant i \leqslant r.$$

Luînd $a = u + (b - a) \bmod m$, este clar că $u \leqslant a < m + u$ și $a \equiv a_i \pmod{m_i}$, $1 \leqslant i \leqslant r$.

De exemplu, fie $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $a_1 = -4$, $a_2 = 8$, $a_3 = -1$ și $u = 0$. Să determinăm prin metoda prezentată la observația de mai sus numărul întreg a, $u \leqslant a < u + m$ astfel încît $a \equiv a_i \pmod{m_i}$, $1 \leqslant i \leqslant 3$. Avem

Scanned with OKEN Scanner

$$m = m_1 m_2 m_3 = 30,$$

$$q_1 = 3 \times 5 = 15, \quad q_2 = 2 \times 5 = 10, \quad q_3 = 2 \times 3 = 6,$$

$$c_1 = q_1^{\varphi(m_1)} = 15^{\varphi(2)} = 15,$$

$$c_2 = q_2^{\varphi(m_2)} = 10^{\varphi(3)} = 10^2 = 100,$$

$$c_3 = q_3^{\varphi(m_3)} = 6^{\varphi(5)} = 6^4 = 1\,296$$

și deci

$$b = a_1 c_1 + a_2 c_2 + a_3 c_3 = (-4) \times 15 + 8 \times 100 + (-1) \times 1\,296 = -556,$$

de unde

$$a = u + (b - u) \bmod m = (-556) \bmod 30 = 14$$

pentru că $-556 = 30 \times (-19) + 14$. Avem $14 = -4 \pmod 2$, $14 \equiv 8 \pmod 3$ și $14 \equiv -1 \pmod 5$.

Dacă luăm $u = 18$, atunci $b - u = -556 - 18 = -574$ și cum

$$-574 = 30 \times (-20) + 26,$$

avem

$$a = 18 + 26 = 44.$$

Deci $44 \equiv -4 \pmod 2$, $44 \equiv 8 \pmod 3$ și $44 \equiv -1 \pmod 5$.

Utilizarea lemei chinezești pentru determinarea lui a în accepțiunea de la observația precedentă presupune că avem o metodă de calcul a lui $\varphi(m)$, unde m este un număr natural >0.

Propoziția 5.4. *Fie m un număr natural astfel încît*

$$m = m_1 m_2 \ldots m_r, \quad (m_i, m_j) = 1 \text{ pentru } i \neq j.$$

Atunci

$$\varphi(m) = \prod_{i=1}^{r} \varphi(m_i).$$

Scanned with OKEN Scanner

În particular, dacă $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, $e_i \geqslant 1$, *este descompunerea în factori primi distincți* ($p_i \neq p_j$ *pentru* $i \neq j$) *a lui* m, *atunci*

$$\varphi(m) = \prod_{i=1}^{r} p_i^{e_i}\left(1 - \frac{1}{p_i}\right) = m \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$

Demonstrație. Pentru $u = 0$, lema chinezească a resturilor arată că aplicația

$$\rho : E \to F,\ \rho(a) = (a \bmod m_1, \dots, a \bmod m_r)$$

stabilește o corespondență bijectivă între mulțimea E a numerelor întregi din intervalul $[0, m)$ și mulțimea F a sistemelor de numere întregi

$$(d_1, d_2, \dots, d_r),\ 0 \leqslant d_i < m_i,\ 1 \leqslant i \leqslant r.$$

Din lema 5.1 rezultă că

$$(a, m) = 1 \Leftrightarrow (a, m_i) = 1,\ 1 \leqslant i \leqslant r.$$

Pentru orice $i = 1, 2, \dots, r$ există $b_i \in \mathbb{Z}$ astfel încît

$$a = m_i b_i + a \bmod m_i,$$

de unde

$$(a, m_i) = 1 \Leftrightarrow (a \bmod m_i, m_i) = 1.$$

Este clar că ρ stabilește o corespondență bijectivă între numerele $a \in E$ cu proprietatea $(a, m) = 1$ și sistemele de numere $(d_1, d_2, \dots, d_r) \in F$ cu proprietatea $(d_i, m_i) = 1$, $1 \leqslant i \leqslant r$. Cum numărul unor asemenea sisteme este evident $\varphi(m_1)\varphi(m_2) \dots \varphi(m_r)$, deducem că

$$\varphi(m) = \varphi(m_1)\varphi(m_2) \dots \varphi(m_r).$$

Scanned with OKEN Scanner

Deoarece $p_i \neq p_j$ pentru $i \neq j$, avem $(p_i, p_j) = 1$ şi, aplicînd lema 5.1, obţinem

$$(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1 \text{ pentru } i \neq j.$$

Întrucît $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ (vezi § 3), ultima afirmaţie din enunţul propoziţiei este acum evidentă.

§ 6. O metodă de înmulţire a numerelor naturale mari

Fie $m_1, m_2 \ldots, m_r$ numere naturale >1 astfel încît $(m_i, m_j) = 1$ pentru $i \neq j$, şi fie $m = m_1 m_2 \ldots m_r$. În tot acest paragraf menţinem aceste ipoteze asupra lui $m_1, m_2, \ldots, m_r$ şi m. Dacă a este un număr întreg din intervalul $[0, m)$ (deci $0 \leqslant a < m$), atunci sistemul de numere naturale

$$(a_1, a_2, \ldots, a_r),$$

unde $a_i = a_i \bmod m_i$, $1 \leqslant i \leqslant r$, va fi numit *reprezentarea modulară* a lui a în sistemul de module $\{m_1, m_2, \ldots, m_r\}$.

Este clar că găsirea reprezentării modulare a unui număr natural este o problemă simplă din punctul de vedere al calculului ce trebuie efectuat: revine la aplicarea algoritmului împărţirii cu rest a lui a prin $m_1, m_2, \ldots, m_r$ respectiv. Mai complicat este să recuperăm numărul a cînd cunoaştem reprezentarea sa modulară. O metodă în acest sens a fost dată la observaţia din § 5. Este clar că această metodă devine foarte anevoioasă cînd modulele $m_1, m_2, \ldots, m_r$ sînt mari. În principiu, trebuie să găsim descompunerea în factori primi a numerelor $m_1, m_2, \ldots, m_r$, pentru a putea calcula numerele $\varphi(m_1), \varphi(m_2), \ldots, \varphi(m_r)$ (vezi propoziţia 5.4) şi apoi să calculăm numerele

$$e_i = \left(\frac{m}{m_i}\right)^{\varphi(m_i)}, \quad 1 \leqslant i \leqslant r.$$

Avantajul metodei de la observaţia menţionată constă în faptul că pentru un sistem de reprezentare modulară $\{m_1, m_2, \ldots, m_r\}$ calculul numerelor e_i, $1 \leqslant i \leqslant r$, trebuie făcut o singură dată.

Scanned with OKEN Scanner

O altă metodă de a recupera un număr natural a cînd este cunoscută reprezentarea sa modulară se bazează pe algoritmul lui Euclid extins şi algoritmul împărţirii cu rest şi este mai avantajoasă decît aceea de la observaţia menţionată.

Expunem în continuare această metodă.

Pentru $i<j$ fie $c_{ij} \in \mathbb{Z}$ astfel încît

$$c_{ij}m_i \equiv 1 \pmod{m_j}.$$

Determinarea celor C_n^2 constante c_{ij}, $i<j$, se poate face cu ajutorul algoritmului lui Euclid extins. Într-adevăr, cum pentru $i<j$ avem $(m_i, m_j) = 1$, cu algoritmul menţionat se determină $h, k \in \mathbb{Z}$ astfel încît $hm_i + km_j = 1$. Luînd $c_{ij} = h$, avem $c_{ij}m_i \equiv 1 \pmod{m_j}$. Putem chiar alege c_{ij} astfel încît $0<c_{ij}<m_j$.

Propoziţia 6.1 (*Garner*). *Fie numerele întregi* $a_1, a_2, \ldots, a_r$. *Dacă*

$$b_1 = a_1 \bmod m_1,$$

$$b_2 = (a_2 - b_1)c_{12} \bmod m_2,$$

$$b_3 = ((a_3 - b_1)c_{13} - b_2)c_{23} \bmod m_3,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$b_r = (\ldots((a_r - b_1)c_{1r} - b_2)c_{2r} \ldots - b_{r-1})c_{r-1}, \bmod m_r$$

şi

$$a = b_r m_{r-1} \ldots m_2 m_1 + \ldots + b_3 m_2 m_1 + b_2 m_1 + b_1,$$

atunci $0 \leqslant a < m$ *şi* $a \equiv a_i \pmod{m_i}$, $1 \leqslant i \leqslant r$.

Demonstraţie. Pentru ca demonstraţia să fie mai uşor de urmărit, să considerăm cazul particular $r = 3$. Folosind faptul că $c_{23}m_2 \equiv 1 \pmod{m_3}$ şi $c_{13}m_1 \equiv 1 \pmod{m_3}$, avem

$$a = b_3m_2m_1 + b_2m_1 + b_1 \equiv [((a_3 - b_1)c_{13} - b_2)c_{23}m_2m_1 +$$

$$+ b_2m_1 + b_1] \equiv [(a_3 - b_1)c_{13}m_1 - b_2m_1 + b_2m_1 + b_1] (\text{mod } m_3) \equiv$$

$$\equiv [a_3 - b_1 + b_1] (\text{mod } m_3) = a_3 (\text{mod } m_3),$$

de unde

$$a \equiv a_3 (\text{mod} m_3).$$

Analog,

$$a = b_3m_2m_1 + b_2m_1 + b_1 \equiv [b_2m_1 + b_1] (\text{mod } m_2) \equiv$$

$$\equiv [(a_2 - b_1)c_{12}m_1 + b_1] (\text{mod } m_2) \equiv [a_2 - b_1 + b_1] (\text{mod } m_2) =$$

$$= a_2 (\text{mod } m_2).$$

În sfîrşit,

$$a = b_3m_2m_1 + b_2m_1 + b_1 \equiv b_1 (\text{mod } m_1) \equiv a_1 (\text{mod } m_1).$$

Cum $0 \leqslant b_i < m_i$, $1 \leqslant i \leqslant 3$, avem

$$m = m_3m_2m_1 \geqslant b_3m_2m_1 + m_2m_1 \geqslant b_3m_2m_1 + b_2m_1 + m_1 >$$

$$> b_3m_2m_1 + b_2m_1 + b_1 \geqslant 0,$$

de unde $0 \leqslant a < m$.

De exemplu, fie $m_1 = 7$, $m_2 = 9$ şi $m_3 = 10$. Se poate arăta că $(m_i, m_j) = 1$ pentru $i \neq j$. Aşadar, putem folosi numerele 7, 9, 10 pentru reprezentarea modulară a numerelor întregi din intervalul $[0, m)$, unde $m = m_1m_2m_3 = 7 \times 9 \times 10 = 630$. Fie $a = 235$. Să găsim reprezentarea modulară a lui 235 în sistemul de module $\{7, 9, 10\}$ şi apoi să-l recuperăm prin metoda expusă la propoziţia 6.1. Din

$$a_1 = a \bmod m_1 = 235 \bmod 7 = 4,$$

$$a_2 = a \bmod m_2 = 235 \bmod 9 = 1,$$

$$a_3 = a \bmod m_3 = 235 \bmod 10 = 5$$

Scanned with OKEN Scanner

rezultă că reprezentarea modulară a numărului $a = 235$ este

$$\rho(a) = (4, 1, 5).$$

Reciproc, să găsim numărul natural a dacă în sistemul de module $\{7, 9, 10\}$ are reprezentarea modulară (4, 1, 5). Trebuie mai întîi să determinăm constantele c_{ij}, $1 \leqslant i < j \leqslant 3$, astfel încît

$$c_{ij} m_i = 1 (\mathrm{mod}\ m_j).$$

Folosind algoritmul lui Euclid extins sau chiar prin încercări ($\hat{c}_{ij}$ este inversul lui $\hat{m}_i$ în inelul $\mathbb{Z}_{mj}$), găsim

$$c_{12} = 4,\ c_{13} = 3,\ c_{23} = 9.$$

Avem

$$b_1 = a_1 \bmod 7 = 4 \bmod 7 = 4,$$

$$b_2 = (a_2 - a_1)c_{12} \bmod 9 = (1 - 4) \times 4 \bmod 9 = (-12) \bmod 9 = 6,$$

$$b = ((a_3 - b_1)c_{13} - b_2)c_{23} \bmod 10 = ((5 - 4) \times 3 - 6) \times 9 \bmod 10 =$$

$$= (-27) \bmod 10 = 3,$$

de unde

$$a = b_3 m_2 m_1 + b_2 m_1 + b_1 = 3 \times 9 \times 7 + 6 \times 7 + 4 = 235.$$

În continuare, vom arăta cum putem, aplicînd metode ale aritmeticii modulare, să reducem efectuarea înmulţirii a două numere naturale mari la înmulţirea de numere naturale mai mici, pentru care se presupune cunoscută o metodă de înmulţire.

Să facem mai întîi o observaţie cu caracter general şi anume că dacă a şi b sînt două numere naturale iar $c = ab$, atunci

$$(c_1, \ldots, c_r) = ((a_1 b_1) \bmod m_1, \ldots, (a_r b_r) \bmod m_r),$$

unde

$$c_i = c \bmod m_i,\ a_i = a \bmod m_i,\ b_i = b \bmod m_i,\ 1 \leqslant i \leqslant r.$$

Scanned with OKEN Scanner

Într-adevăr, există $u_i, v_i, w_i \in \mathbb{Z}$ astfel încît

$$a = m_i u_i + a_i,\ b = m_i v_i + b_i,\ c = m_i w_i + c_i,\ 1 \leqslant i \leqslant r.$$

Cum

$$c = ab = m_i (m_i u_i v_i + a_i v_i + u_i b_i) + a_i b_i,$$

rezultă că $c \equiv a_i b_i (\mathrm{mod}\ m_i)$, de unde

$$c_i = c \bmod m_i = (a_i b_i) \bmod m_i,\ 1 \leqslant i \leqslant r.$$

Presupunem că $a, b \in [0, m)$, $m = m_1 m_2 \ldots m_r$, astfel încît $c = ab$ să fie tot în intervalul $[0, m)$. Cu siguranţă aşa se întîmplă cînd $a < [\sqrt[]{m}]$ şi $b < [\sqrt[]{m}]$, deoarece

$$a < [\sqrt[]{m}] \text{ şi } b < [\sqrt[]{m}] \Rightarrow ab < m.$$

Dacă $c = ab \in [0, m)$, putem imagina următoarea metodă de calcul al produsului ab cînd avem deja o metodă de înmulţire a numerelor naturale $< \max \{m_1, \ldots, m_r\}$:

P_1. Calculăm $a_i = a \bmod m_i$; $b_i = b \bmod m_i$, $1 \leqslant i \leqslant r$.

P_2. Calculăm $a_i b_i$, $1 \leqslant i \leqslant r$, conform metodei presupuse cunoscută.

P_3. Calculăm $c_i = (a_i b_i) \bmod m_i$, $1 \leqslant i \leqslant r$.

P_4. Găsim unicul număr natural $c \in [0, m)$ astfel încît

$$c \bmod m_i = c_i, \quad 1 \leqslant i \leqslant r.$$

Atunci, numărul natural c astfel determinat este produsul ab după cum rezultă din lema chinezească a resturilor şi din consideraţiile precedente.

În esenţă, dacă pentru paşii P_1, P_3 şi P_4 dispunem de procedee satisfăcătoare de execuţie, atunci metoda expusă reduce înmulţirea numerelor naturale $< [\sqrt[]{m}]$ la înmulţirea numerelor naturale $< \max \{m_1, \ldots, m_r\}$.

Scanned with OKEN Scanner

De exemplu, fie $m_1 = 7$, $m_2 = 9$, $m_3 = 10$. Avem, $m = m_1 m_2 m_3 = 630$. Presupunem cunoscută tabla înmulțirii numerelor naturale $\leqslant 9 < \max\{7, 9, 10\}$ și să verificăm pe un exemplu că putem folosi metoda expusă pentru a efectua produsul numerelor naturale $\leqslant [\sqrt{630}] = 25$. Fie $a = 17$ și $b = 23$. Executînd instrucțiunea P_1, găsim

$$\rho(a) = (3, 8, 7) \quad \text{și} \quad \rho(b) = (2, 5, 3).$$

La pasul P_2, conform tablei înmulțirii numerelor $\leqslant 9$, găsim

$$a_1 b_1 = 3 \times 2 = 6, \quad a_2 b_2 = 8 \times 5 = 40, \quad a_3 b_3 = 7 \times 3 = 21.$$

Acum, prin pasul P_3, găsim reprezentarea modulară a produsului $c = ab$, anume :

$$c_1 = (a_1 b_1) \bmod m_1 = 6 \bmod 7 = 6,$$

$$c_2 = (a_2 b_2) \bmod m_2 = 40 \bmod 9 = 4,$$

$$c_3 = (a_3 b_3) \bmod m_3 = 21 \bmod 10 = 1,$$

deci

$$\rho(c) = (6, 4, 1).$$

Folosind metoda de la propoziția 6.1 (vezi și primul exemplu), găsim $ab = c = 391$.

Acest exemplu ilustrează metoda propusă, dar nu lasă să se întrevadă o economie de calcule pentru efectuarea produsului a două numere. În realitate, metoda prezintă avantaje cînd se aplică la numere foarte mari. Mai mult, dacă folosim reprezentarea binară a numerelor și module de forma $2^e - 1$, $e > 1$, atunci se obțin avantaje substanțiale.

Lema 6.2. *Fie e, f și g trei numere naturale $\neq 0$. Atunci*

$$2^e \equiv 2^f \pmod{2^g - 1} \Leftrightarrow e \equiv f \pmod{g}.$$

Demonstrație. Fie $q, r \in \mathbb{N}$ astfel încît

$$e = gq + r, \quad 0 \leqslant r < g.$$

De exemplu, fie $m_1 = 7$, $m_2 = 9$, $m_3 = 10$. Avem, $m = m_1 m_2 m_3 = 630$. Presupunem cunoscută tabla înmulțirii numerelor naturale $\leqslant 9 < \max\{7, 9, 10\}$ și să verificăm pe un exemplu că putem folosi metoda expusă pentru a efectua produsul numerelor naturale $\leqslant [\sqrt{630}] = 25$. Fie $a = 17$ și $b = 23$. Executînd instrucțiunea P_1, găsim

$$\rho(a) = (3, 8, 7) \quad \text{și} \quad \rho(b) = (2, 5, 3).$$

La pasul P_2, conform tablei înmulțirii numerelor $\leqslant 9$, găsim

$$a_1 b_1 = 3 \times 2 = 6, \quad a_2 b_2 = 8 \times 5 = 40, \quad a_3 b_3 = 7 \times 3 = 21.$$

Acum, prin pasul P_3, găsim reprezentarea modulară a produsului $c = ab$, anume :

$$c_1 = (a_1 b_1) \bmod m_1 = 6 \bmod 7 = 6,$$

$$c_2 = (a_2 b_2) \bmod m_2 = 40 \bmod 9 = 4,$$

$$c_3 = (a_3 b_3) \bmod m_3 = 21 \bmod 10 = 1,$$

deci

$$\rho(c) = (6, 4, 1).$$

Folosind metoda de la propoziția 6.1 (vezi și primul exemplu), găsim $ab = c = 391$.

Acest exemplu ilustrează metoda propusă, dar nu lasă să se întrevadă o economie de calcule pentru efectuarea produsului a două numere. În realitate, metoda prezintă avantaje cînd se aplică la numere foarte mari. Mai mult, dacă folosim reprezentarea binară a numerelor și module de forma $2^e - 1$, $e > 1$, atunci se obțin avantaje substanțiale.

Lema 6.2. *Fie e, f și g trei numere naturale $\neq 0$. Atunci*

$$2^e \equiv 2^f \pmod{2^g - 1} \Leftrightarrow e \equiv f \pmod{g}.$$

Demonstrație. Fie $q, r \in \mathbb{N}$ astfel încît

$$e = gq + r, \quad 0 \leqslant r < g.$$

Scanned with OKEN Scanner

Avem

$$(2^q)^q - 1 = (2^q - 1)(1 + 2^q + \ldots + 2^{(q-1)q}),$$

de unde

$$2^{qq} \equiv 1 \pmod{2^q - 1}.$$

Înmulţind ultima congruenţă cu 2^r, se obţine

$$2^{qq+r} \equiv 2^r \pmod{2^q - 1}, \tag{5.8}$$

deci

$$2^e \equiv 2^{e \bmod q} \pmod{2^q - 1}. \tag{5.9}$$

Analog,

$$2^f \equiv 2^{f \bmod q} \pmod{2^q - 1}.$$

Dacă $e \equiv f \pmod g$, atunci $e \bmod g = f \bmod g$ şi folosind (5.8) şi (5.9) deducem

$$2^e \equiv 2^f \pmod{2^q - 1}.$$

Reciproc, dacă ultima congruenţă are loc, atunci din (5.8) şi (5.9) rezultă

$$2^{e \bmod q} \equiv 2^{f \bmod q} \pmod{2^q - 1};$$

deci

$$(2^q - 1) \mid 2^{e \bmod q} - 2^{f \bmod q}$$

Deoarece $0 \leqslant e \bmod g < q$ şi $0 \leqslant f \bmod g < g$, rezultă $e \bmod g = f \bmod g$, de unde $e \equiv f \pmod g$.

Lema 6.3. *Dacă e şi f sînt două numere naturale nenule, atunci*

$$(2^e - 1, 2^f - 1) = 2^{(e,f)} - 1.$$

În particular, dacă $(e, f) = 1$, atunci

Scanned with OKEN Scanner

$$(2^e - 1, 2^f - 1) = 1.$$

Demonstrație. Fie $q, r \in \mathbb{Z}$ astfel încît $e = fq + r$, $0 \leqslant r < f$. Din $e \equiv r \pmod f$ și din lema 6.2 rezultă

$$2^e \equiv 2^r \pmod{2^f - 1},$$

de unde

$$2^e - 1 \equiv 2^r - 1 \pmod{2^f - 1}.$$

Cum $0 \leqslant r < f$, avem $0 \leqslant 2^r - 1 < 2^f - 1$, deci $2^r - 1$ este restul împărțirii lui $2^e - 1$ prin $2^f - 1$. Să mai observăm că

$$2^r - 1 = 0 \Leftrightarrow r = 0. \tag{5.10}$$

Dacă $r \neq 0$, reluăm calculul precedent după substituția

$$e \leftarrow f,\ f \leftarrow r.$$

Se execută astfel în paralel algoritmul lui Euclid pentru cuplurile e, f, respectiv $2^e - 1$, $2^f - 1$. Conform cu (5.10), ultimul rest diferit de zero se obține simultan pentru ambele cupluri de numere. Dar (e, f) este ultimul rest diferit de zero în algoritmul lui Euclid pentru cuplul e, f. Rezultă că $2^{(e,f)} - 1$ este ultimul rest diferit de zero în algoritmul lui Euclid pentru cuplul $2^e - 1$, $2^f - 1$, de unde

$$(2^e - 1, 2^f - 1) = 2^{(e,f)} - 1.$$

Să definim recurent numerele $q_0, q_1, \ldots$ prin

$$q_0 = 1,\ q_{k+1} = 3q_k - 1.$$

Pentru orice $k \geqslant 0$, avem

$$q_k = \frac{1}{2}(3^k + 1).$$

Scanned with OKEN Scanner

Într-adevăr,

$$\frac{1}{2}(3^0 + 1) = 1 = q_0$$

şi dacă

$$q_{k-1} = \frac{1}{2}(3^{k-1} + 1),$$

atunci

$$q_k = 3q_{k-1} - 1 = \frac{3}{2}(3^{k-1} + 1) - 1 = \frac{1}{2}(3^k + 1)$$

şi afirmaţia făcută este astfel demonstrată prin inducţie.

Lema 6.4. *Numerele* $m_1 = 2^{6q_k - 1} - 1$, $m_2 = 2^{6q_k + 1} - 1$, $m_3 = 2^{6q_k + 2} - 1$, $m_4 = 2^{6q_k + 3} - 1$, $m_5 = 2^{6q_k + 5} - 1$, $m_6 = 2^{6q_k + 7}$ *sînt relativ prime în perechi* [*deci* $(m_i, m_j) = 1$ *pentru* $i \neq j$].

Demonstraţie. Conform lemei 6.3 este suficient să arătăm că numerele

$$6q_k - 1,\ 6q_k + 1,\ 6q_k + 2,\ 6q_k + 3,\ 6q_k + 5,\ 6q_k + 7 \quad (5.11)$$

sînt relativ prime în perechi. Un divizor comun prim p pentru două din numerele (5.11) este divizor şi al valorii absolute a diferenţei lor. Dar diferenţele în valoarea absolută posibile ale perechilor de numere din lista respectivă sînt

$$2,\ 3,\ 4,\ 6,\ 8,\ 1,\ 5$$

şi divizorii primi posibili ai acestor numere sînt

$$2,\ 3,\ 5.$$

Scanned with OKEN Scanner

Afirmaţia din enunţul lemei este adevărată dacă arătăm că fiecare dintre numerele prime 2, 3 şi 5 divide cel mult unul din numerele listei (5.11). Este clar că 2 divide doar pe $6q_k + 2$ iar 3 divide doar pe $6q_k + 3$. Să observăm că

$$q_k \not\equiv 3 \pmod 5,$$

deoarece în caz contrar

$$q_k = 3 + 5h, \quad h \in \mathbb{Z},$$

de unde

$$3^k + 1 = 6 + 10\,h,$$

deci

$$3^k = 5\,(1 + 2h).$$

Rezultă că $5 \mid 3$ (contradicţie !).

Dacă 5 divide pe $6q_k + 2$, atunci 5 divide pe

$$q_k - 3 = (6q_k + 2) - 5q_k - 5,$$

deci $q_k \equiv 3 \pmod 5$, ceea ce s-a văzut că nu este posibil. Deci 5 nu divide pe $6q_k + 2$ şi atunci nu divide nici pe $6q_k + 7 = (6q + 2) + 5$. În sfîrşit, 5 nu poate divide simultan două dintre numerele $6q_k - 1$, $6q_k + 1$, $6q_k + 3$ şi $6q + 5$, întrucît diferenţele posibile dintre acestea sînt 2, 4 şi 6. Deci 5 divide cel mult un număr din lista (5.11).

Lema 6.5. *Fie numerele naturale* e_1, e_2, e_3, e_4, e_5 *şi* e_6 *astfel încît* $e_1 < e_2 < \ldots < e_6$. *Atunci*

$$\prod_{i=1}^{6} (2^{e_i} - 1) > 2^{e_1 + \ldots + e_6} - 2^{5e_6 + 3} - 2^{3e_6 + 7} - 2^{e_6 + 3}.$$

Demonstraţie. Dezvoltăm produsul din enunţ şi clasificăm termenii negativi ai dezvoltării în :

1° C_6^5 termeni de forma $-2^{e_i+e_j+e_k+e_s+e_t}$, $1 \leqslant i<j<k<s<t \leqslant 6$;

2° C_6^3 termeni de forma $-2^{e_i+e_j+e_k}$, $1 \leqslant i<j<k \leqslant 6$;

3° C_6^1 termeni de forma -2^{e_i}, $1 \leqslant i \leqslant 6$.

Termenii de tip 1°, 2° şi 3° se minorează respectiv cu -2^{5e_6}, -2^{3e_6}, -2^{e_6}. Mai avem

$$C_6^1 = C_6^5 = 6<2^3,\ C_6^3 = 120<2^7.$$

Eliminînd din dezvoltarea produsului $\prod_{i=1}^{6}(2^{e_i}-1)$ toţi termenii pozitivi mai puţin $2^{e_1+e_2+\ldots+e_6}$ şi minorînd termenii negativi, obţinem

$$\prod_{i=1}^{6}(2^{e_i}-1)>2^{e_1+\ldots+e_6}-C_6^5\,2^{5e_6}-C_6^3\,2^{3e_6}-C_6^1\,2^{e_6}>$$

$$>2^{e_1+\ldots+e_6}-2^{5e_6+3}-2^{3e_6+7}-2^{e_6+3}.$$

Corolarul 6.6. *Dacă* $m_1, m_2, \ldots, m_6$ *sînt numerele de la lema* 6.4, $p_k = 18q_k + 8$ *şi* $m = m_1 m_2 \ldots m_6$, *atunci*

$$m>2^{2p_k},\quad k = 0, 1, 2, \ldots$$

Demonstraţie. Conform lemei precedente, avem

$$m>2^{36q_k+17}-2^{30q_k+38}-2^{18q_k+28}-2^{6q_k+10},$$

de unde se obţine uşor că $m>2^{2p_k}$.

Expunem acum metoda lui Schönhage pentru înmulţirea numerelor naturale mari. Numerele le presupunem date în sistemul de numeraţie binar. Metoda dă o procedură de înmulţire a numerelor cu $q_k = 18q_k + 8$ cifre binare, folosind reprezentarea lor modulară în sistemul de

Scanned with OKEN Scanner

module $\{m_1, m_2, \ldots, m_6\}$ din lema 6.4 și presupunînd deja elaborată o procedură de înmulțire a numerelor naturale cu $p_{k-1} = 18q_{k-1} + 8$ cifre binare. Cum $m > 2^{2p_k}$ și un număr cu p_k cifre binare este mai mic decît 2^{p_k}, rezultă că produsul de două numere cu p_k cifre binare aparține intervalului $[0, m)$. Calculul produsului a două numere a și b cu p_k cifre binare se face cu instrucțiunile P_1, P_2, P_3 și P_4. De observat că

$$a_i = a \bmod m_i, \qquad b_i = b \bmod m_i, \qquad 1 \leqslant i \leqslant 6,$$

sînt numere $< 2^{6q_k+7} = 2^{18p_{k-1}+1} < 2^{p_k-1}$, deci sînt numere cu cel mult p_{k-1} cifre binare. Așadar, produsul $a_i b_i$ la pasul P_2 se face conform procedurii de înmulțire a numerelor cu p_{k-1} cifre binare, procedură presupusă cunoscută. Conversiunea numerelor de la reprezentarea modulară la cea binară (pasul P_4) se face conform metodei date de propoziția 6.1.

Presupunînd elaborată o procedură de înmulțire a numerelor cu $p_0 = 18q_0 + 8 = 26$ cifre binare, metoda Schönhage dă o procedură de înmulțire a numerelor cu $p_1 = 18q_1 + 8 = 36 + 8 = 44$ cifre binare, apoi o procedură de înmulțire a numerelor cu $p_2 = 18q_2 + 8 = 98$ cifre binare etc.

Scanned with OKEN Scanner

Rezolvarea în numere întregi a sistemelor de ecuații liniare

§ 1. Matrice elementare

Reamintim mai întîi cîteva definiţii şi rezultate în legătură cu matricele şi determinanţii.

Fie m şi n două numere întregi pozitive. Prin *matrice* de tip $m \times n$ peste inelul $\mathbb{Z}$ se înţelege un tablou A cu m linii şi n coloane

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

unde $a_{ij} \in \mathbb{Z}$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, sînt numite *elementele* lui A. Numărul a_{ij} de la intersecţia liniei i cu coloana j va fi reperat spunînd că este elementul lui A din poziţia (i, j). Dacă tipul matricei A este subînţeles, vom scrie condensat $A = (a_{ij})$. Dacă $A = (a_{ij})$ şi $B = (b_{ij})$ sînt matrice de tip $m \times n$, atunci

$$A = B \overset{\text{def}}{\Leftrightarrow} a_{ij} = b_{ij},\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n.$$

Scanned with OKEN Scanner

Se definește adunarea matricelor de același tip prin formula

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} \overset{\text{def}}{=} \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \dots & \dots & \dots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

iar produsul unei matrice de tipul $m \times n$ cu o matrice de tipul $n \times p$ ca fiind matricea de tipul $m \times p$ definită prin formula

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \dots & b_{1p} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{np} \end{pmatrix} \overset{\text{def}}{=} \begin{pmatrix} c_{11} & \dots & c_{1p} \\ \dots & \dots & \dots \\ c_{m1} & \dots & c_{mp} \end{pmatrix},$$

unde

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}\, b_{kj},$$

$$1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant p.$$

Notăm $M_n(\mathbb{Z})$ mulțimea tuturor matricelor de tipul $n \times n$ peste $\mathbb{Z}$, numite *matrice pătrate* de ordin n peste $\mathbb{Z}$. Să observăm că adunarea și înmulțirea matricelor sînt operații algebrice pe mulțimea $M_n(\mathbb{Z})$.

Adunarea matricelor din $M_n(\mathbb{Z})$ este asociativă și comutativă, admite ca element de efect nul matricea

$$O = \begin{pmatrix} 0 & 0 \dots 0 \\ 0 & 0 \dots 0 \\ \dots & \dots \\ 0 & 0 \dots 0 \end{pmatrix},$$

numită *matricea zero*, și orice matrice A admite opusă față de operația de adunare a matricelor, anume

$$-A = \begin{pmatrix} -a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & -a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -a_{n1} & -a_{n2} & \dots & -a_{nn} \end{pmatrix}.$$

Scanned with OKEN Scanner

Înmulțirea matricelor este asociativă și distributivă față de operația de adunare și admite ca element de efect nul matricea

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

numită *matricea unitate* de ordin n.

Rezultă că mulțimea $M_n(\mathbb{Z})$ formează inel față de operațiile de adunare și înmulțire a matricelor, numit *inelul matricelor pătrate* de ordin n peste $\mathbb{Z}$.

Dacă $A = (a_{ij}) \in M_n(\mathbb{Z})$, definim *determinantul* lui A astfel :

$$\det A = \sum_{\sigma} \varepsilon_\sigma \, a_{1\sigma(1)} \, a_{2\sigma(2)} \dots a_{n\sigma(n)},$$

unde suma se face după cele $n!$ permutări ale numerelor $1, 2, \dots, n$,

$$\sigma = \begin{pmatrix} 1 & 2 \dots & n \\ \sigma(1) & \sigma(2) \dots & \sigma(n) \end{pmatrix}$$

iar ε_σ, numit *signatura* lui σ, este egal cu 1 cînd σ este permutare pară și egal cu -1 cînd σ este permutare impară.

Dacă notăm numărul $(-1)^{i+j}$ înmulțit cu determinantul matricei de ordin $n-1$ obținute eliminînd din matricea $A = (a_{ij})$ linia i și coloana j, cu A_{ij}, numit *complementul algebric* al elementului a_{ij}, avem :

$$a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in} = \det A, \; 1 \leqslant i \leqslant n,$$

$$a_{1j}A_{1j} + a_{2j}A_{2j} + \dots + a_{nj}A_{nj} = \det A, \; 1 \leqslant j \leqslant n$$

De asemenea, pentru $i \neq j$ avem

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \dots + a_{in}A_{jn} = 0$$

și

$$a_{1i}A_{1j} + a_{2i}A_{2j} + \dots + a_{ni}A_{nj} = 0.$$

Scanned with OKEN Scanner

În sfîrșit, amintim că pentru orice $A, B \in M_n(\mathbb{Z})$ avem

$$\det AB = \det A \cdot \det B.$$

O matrice $U \in M_n(\mathbb{Z})$ se numește *unimodulară* dacă $\det U = \pm 1$. Vom nota cu $GL_n(\mathbb{Z})$ grupul unităților inelului $M_n(\mathbb{Z})$, numit grupul general liniar de ordin n al lui $\mathbb{Z}$. Evident,

$U \in GL_n(Z) \Leftrightarrow$ există $V \in M_n(\mathbb{Z})$ astfel încît $UV = VU = E$.

Propoziția 1.1. *Pentru o matrice $U \in M_n(\mathbb{Z})$, $U = (u_{ij})$ următoarele afirmații sînt echivalente:*

1) $U \in GL_n(\mathbb{Z})$;

2) *U este unimodulară.*

Demonstrație. 1)⇒2). Dacă $U \in GL_n(\mathbb{Z})$, există $V \in M_n(\mathbb{Z})$ astfel încît $UV = VU = E$. Rezultă că

$$1 = \det E = \det (UV) = \det U \cdot \det V.$$

Cum $\det U \in \mathbb{Z}$ și $\det V \in \mathbb{Z}$, deducem că $\det U = \pm 1$, deci U este unimodulară.

2) ⇒ 1). Fie U o matrice unimodulară. Cum $\det U = \pm 1 \neq 0$, rezultă că U este inversabilă în inelul $M_n(\mathbb{Q})$. Avem

$$U^{-1} = \frac{1}{\det U} \begin{pmatrix} U_{11} & U_{21} & \dots & U_{n1} \\ U_{12} & U_{22} & \dots & U_{n2} \\ \dots & \dots & \dots & \dots \\ U_{1n} & U_{2n} & \dots & U_{nn} \end{pmatrix},$$

unde U_{ij} este complementul algebric al elementului u_{ij}. Dacă $U \in M_n(\mathbb{Z})$, rezultă că $U_{ij} \in \mathbb{Z}$. Dar $\det U = \pm 1$, de unde $U^{-1} \in M_n(\mathbb{Z})$. Luînd $V = U^{-1} \in M_n(\mathbb{Z})$, avem $UV = VU = E$, deci $U \in GL_n(\mathbb{Z})$.

Fie $i, j, \lambda \in \mathbb{Z}$, $i \neq j$, $1 \leqslant i, j \leqslant n$. Vom nota cu $T_{ij}(\lambda)$ matricea pătrată de ordin n care are 1 pe diagonala principală, λ la intersecția liniei i cu coloana j și 0 în cele-

Scanned with OKEN Scanner

lalte poziţii :

$$T_{ij}(\lambda) = \begin{array}{c} \begin{array}{cccccc} & & & j & & \end{array} \\ \left(\begin{array}{cccc|cccc} 1 & & & & & & & \\ & 1 & & & & & 0 & \\ & & \cdot & & & & & \\ \hline & & & \cdot & \lambda & & & \\ & & & & & \cdot & & \\ & 0 & & & & & \cdot & \\ & & & & & & & 1 \end{array}\right) \end{array} \begin{array}{c} \\ \\ \\ i \\ \\ \\ \\ \end{array}$$

Evident, det $T_{ij}(\lambda) = 1$, de unde rezultă că $T_{ij}(\lambda) \in GL_n(\mathbb{Z})$. Matricele $T_{ij}(\lambda)$, $1 \leqslant i, j \leqslant n$, $i \neq j$, $\lambda \in \mathbb{Z}$, se numesc *elementare*.

Propoziţia 1.2. *Fie $A = (a_{ij})$ o matrice cu m linii şi n coloane, cu elemente $a_{ij} \in \mathbb{Z}$.*

1) *Dacă $T_{ij}(\lambda)$ este o matrice elementară de ordin m, atunci matricea $T_{ij}(\lambda)A$ se obţine din A adunînd la elementele liniei i pe cele ale liniei j înmulţite cu λ.*

2) *Dacă $T_{ij}(\lambda)$ este o matrice elementară de ordin n, atunci matricea $AT_{ij}(\lambda)$ se obţine din A, adunînd la elementele coloanei j pe cele ale coloanei i înmulţite cu λ.*

Demonstraţia acestei propoziţii rezultă direct din definiţia înmulţirii matricelor.

Astfel, dacă $m = 3$ şi $n = 4$,

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix} \text{ şi } T_{23}(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix},$$

atunci

$$T_{23}(\lambda)A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} + \lambda a_{31} & a_{22} + \lambda a_{32} & a_{22} + \lambda a_{33} & a_{24} + \lambda a_{34} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix},$$

după cum rezultă efectuînd produsul $T_{23}(\lambda)A$.

Introducem încă matricele D_i, $1 \leqslant i \leqslant n$, care se obţin din matricea unitate E înlocuind elementul 1 al matricei E din linia şi coloana i cu -1 :

$$D_i = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ \end{matrix}, \quad 1 \leqslant i \leqslant n.$$

Cum $\det D_i = -1$, avem $D_i \in GL_n(\mathbb{Z})$, $1 \leqslant i \leqslant n$. Vom include printre matricele elementare şi matricele D_i, $1 \leqslant i \leqslant n$. Se demonstrează imediat :

Propoziţia 1.3. *Fie $A = (a_{ij})$ o matrice cu m linii şi n coloane, cu elemente $a_{ij} \in \mathbb{Z}$.*

1) *Dacă D_i are ordinul m, atunci matricea D_iA se obţine din A înmulţind elementele liniei i cu -1.*

2) *Dacă D_i are ordinul n, atunci matricea AD_i se obţine din A înmulţind elementele coloanei i cu -1.*

Matricele pătrate P_{ij}, $i < j$, de forma

$$P_{ij} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & 1 & \\ & & & 1 & \ddots & \\ & & & 1 & 0 & \\ & & & & & 1 \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ i \\ \\ j \\ \\ \\ \end{matrix}, \quad \begin{matrix} \\ \\ \\ i \\ \\ j \\ \\ \\ \end{matrix}$$

elementele nespecificate fiind egale cu 0, se numesc *matrice de transpoziţie.*

Scanned with OKEN Scanner

Propoziția 1.4. *Fie $A = (a_{ij})$ o matrice cu m linii și n coloane, cu elemente $a_{ij} \in \mathbb{Z}$.*

1) *Dacă P_{ij} are ordinul m, atunci matricea $P_{ij}A$ se obține din A permutînd linia i cu linia j.*

2) *Dacă P_{ij} are ordinul n, atunci matricea AP_{ij} se obține din A permutînd coloana i cu coloana j.*

Demonstrația rezultă, din nou, direct din definiția înmulțirii matricelor.

Astfel, decă $m = 3$ și $n = 4$, atunci

$$AP_{23} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{14} & a_{13} & a_{12} \\ a_{21} & a_{24} & a_{23} & a_{22} \\ a_{31} & a_{34} & a_{33} & a_{32} \end{pmatrix}$$

Propoziția 1.5. *Pentru orice $i < j$ avem*

$$P_{ij} = S_i T_{ji}(1)\, T_{ij}(-1)\, T_{ji}(1).$$

În particular, $\det P_{ij} = -1$ *și deci* $P_{ij} \in GL_n(\mathbb{Z})$.

Demonstrație. Direct din definiția înmulțirii matricelor se obține

$$P_{ij} = S_i T_{ij}(1)\, T_{ij}(-1)\, T_{ji}(1).$$

Avem

$$\det P_{ij} = \det S_i \cdot \det T_{ij}(1) \cdot \det T_{ij}(-1) \cdot \det T_{ji}(1) =$$
$$= (-1) \times 1 \times 1 \times 1 = -1.$$

Înmulțirea la stînga sau la dreapta a unei matrice A cu o matrice elementară $T_{ij}(\lambda)$ sau D_i se numește *transformare elementară* asupra lui A.

Să observăm că înmulțirea lui A cu o matrice de transpoziție P_{ij} revine, conform propoziției 1.5, la a efectua asupra lui A o secvență de patru transformări elementare.

Scanned with OKEN Scanner

Vom nota cu $M_{m\times n}(\mathbb{Z})$ mulțimea tuturor matricelor cu m linii și n coloane, cu elemente din inelul $\mathbb{Z}$, numite încă *matrice de tip* $m \times n$ cu elemente din $\mathbb{Z}$.

Fie $A, B \in M_{m\times n}(\mathbb{Z})$. Spunem că *$A$ este aritmetic echivalentă cu B*, și scriem $A \sim B$, dacă există $U \in GL_m(\mathbb{Z})$ și $V \in GL_n(\mathbb{Z})$ astfel încît

$$UAV = B.$$

Se verifică imediat că

$A \sim A$, oricare ar fi $A \in M_{m\times n}(\mathbb{Z})$;

$A \sim B \Rightarrow B \sim A$;

$A \sim B$ și $B \sim C \Rightarrow A \sim C$,

deci $\sim$ este o relație de echivalență pe mulțimea $M_{m\times n}(\mathbb{Z})$.

Lema 2.1. *Oricare ar fi $A \in M_{m\times n}(\mathbb{Z})$, există $0 \leqslant r \leqslant \min\{m, n\}$ și $d_1, \ldots, d_r \in \mathbb{Z}$, $d_i > 0$, $1 \leqslant i \leqslant r$, astfel încît*

$$A \sim \begin{pmatrix} d_1 & & & & 0 \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_r & \\ 0 & & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

Demonstrație. Pentru orice matrice $A \in M_{m\times n}(\mathbb{Z})$ definim

$$\varphi(A) = 0, \text{ dacă } A = 0,$$

și

$$\varphi(A) = \min\{|a_{ij}| \mid a_{ij} \neq 0\}, \text{ dacă } A \neq 0.$$

Lema este evidentă dacă $A = 0$. Presupunem $A \neq 0$ și că lema este adevărată pentru matricele B de tip $m \times n$ cu $\varphi(B) < \varphi(A)$ și pentru matricele de tip $(m-1) \times$

Scanned with OKEN Scanner

$\times (n-1)$. Evident, există i_0 și j_0, $1 \leqslant i_0 \leqslant m$, $1 \leqslant j_0 \leqslant n$, astfel încît

$$\varphi(A) = |a_{i_0 j_0}|.$$

Prin permutări de linii și coloane se poate aduce $a_{i_0 j_0}$ în poziția (1, 1) (mai precis, avem $A \sim P_{1 i_0} A P_{1 j_0}$). Putem presupune, deci, că $\varphi(A) = |a_{11}|$. Înmulțind cu D_1 matricea A cînd $a_{11} < 0$, putem presupune chiar că $a_{11} > 0$.

Cazul 1. Presupunem că $a_{11} | a_{1j}$, $2 \leqslant j \leqslant n$ și $a_{11} | a_{i1}$, $2 \leqslant i \leqslant m$. Există q_{1j}, $q_{i1} \in \mathbb{Z}$, astfel încît

$$a_{1j} = a_{11} q_{1j}, \quad 2 \leqslant j \leqslant n,$$

$$a_{i1} = a_{11} q_{i1}, \quad 2 \leqslant i \leqslant m.$$

Adunînd la coloanele $2, 3, \ldots, n$ coloana întîi a lui A înmulțită respectiv cu $-q_{12}, -q_{13}, \ldots, -q_{1n}$ și procedînd analog pentru linii, obținem

$$A \sim \begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix},$$

unde A' este o matrice de tip $(m-1) \times (n-1)$ peste $\mathbb{Z}$. Conform ipotezei inducției, există $U' \in GL_{m-1}(\mathbb{Z})$ și $V' \in GL_{n-1}(\mathbb{Z})$ astfel încît

$$U'A'V' = \begin{pmatrix} d_2 & & & 0 \\ & \ddots & & \\ & & d_r & \\ & & & \ddots \\ 0 & & & 0 \end{pmatrix},$$

unde $d_i > 0$, $2 \leqslant i \leqslant r$.

Definind

$$U = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 \\ 0 & V' \end{pmatrix}, \quad d_1 = a_{11},$$

Scanned with OKEN Scanner

avem $U \in GL_m(\mathbb{Z})$, $V \in GL_n(\mathbb{Z})$ și

$$A \sim U \begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix} V = \begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & 0 & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

Cazul 2. Presupunem că există înprima linie sau prima coloană a lui A un element ce nu se divide prin a_{11}. Pentru a face o alegere, presupunem că a_{1j_0}, $2 \leqslant j_0 \leqslant n$, nu se divide prin a_{11}. Avem

$$a_{1j_0} = a_{11} q_{1j_0} + r_{1j_0}, \quad 0 < r_{1j_0} < a_{11}.$$

Adunînd la coloana j_0 a matricei A coloana întîi înmulțită cu $-q_{1j_0}$, se obține o matrice $B \sim A$ care are în poziția $(1, j_0)$ elementul r_{1j_0}. Avem

$$\varphi(B) \leqslant r_{1j_0} < a_{11} = \varphi(A).$$

Conform ipotezei inducției, B este echivalentă cu o matrice de forma celei din enunțul lemei și deci A are aceeași proprietate.

Observație. În lema precedentă am arătat că orice matrice $A \in M_{m \times n}(\mathbb{Z})$ este echivalentă cu o matrice diagonală, cu numerele de pe diagonală nenegative. Analizînd demonstrația lemei, se observă că matricea diagonală cu care A este echivalentă se obține aplicînd asupra lui A un număr finit de transformări elementare, ceea ce revine la a înmulți matricea A la stînga și dreapta cu un număr finit de matrice elementare.

Lema 2.2. *Orice matrice unimodulară $U \in GL_n(\mathbb{Z})$ este egală cu produsul unui număr finit de matrice elementare.*

Demonstrație. Conform observației de la lema precedentă, există matricele elementare $R_1, \ldots, R_s, Q_1, \ldots, Q_t$,

astfel încît

$$R_s \dots R_1 \cdot UQ_1 \dots Q_t = D = \begin{pmatrix} d_1 & & & & \\ & d_2 & & \mathbf{0} & \\ & & \ddots & & \\ & & & d_r & \\ & \mathbf{0} & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

Cum

$$1 = |\det U| = \det D,$$

rezultă că $\det D \neq 0$, deci $r = n$. Din $d_i > 0$ $1 \leqslant i \leqslant r = n$ şi $d_1 d_2 \dots d_n = 1$ rezultă că $d_1 = d_2 = \dots = d_n = 1$. Deci $D = E$ şi avem

$$U = R_1^{-1} \dots R_s^{-1} Q_t^{-1} \dots Q_1^{-1}.$$

Din $T_{ij}^{-1}(\lambda) = T_{ij}(-\lambda)$ şi $D_i^{-1} = D_i$ rezultă că matricele R_i^{-1}, Q_j^{-1} sînt elementare, deci U este produs finit de matrice elementare.

Lema 2.3. *Oricare ar fi* $a, b \in \mathbb{Z}$, *avem*

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} (a, b) & 0 \\ 0 & [a, b] \end{pmatrix}.$$

Demonstraţie. Fie $d = (a, b)$ şi $a_1, b_1 \in \mathbb{Z}$ astfel încît $a = da_1$, $b = db_1$. Există $h, k \in \mathbb{Z}$ astfel încît

$$d = ha + kb,$$

de unde

$$1 = ha_1 + kb_1.$$

Definim matricele :

$$U = \begin{pmatrix} 1 & 1 \\ -kb_1 & ha_1 \end{pmatrix}, \qquad V = \begin{pmatrix} h & -b_1 \\ k & a_1 \end{pmatrix}.$$

Scanned with OKEN Scanner

Deoarece $\det U = \det V = ha_1 + kb_1 = 1$, rezultă că $U,\ V \in GL_2(\mathbb{Z})$. Ţinînd seama de faptul că $ab = (a, b) \cdot [a, b]$, obţinem

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim U \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} V = \begin{pmatrix} (a, b) & 0 \\ 0 & [a, b] \end{pmatrix}.$$

Sîntem acum pregătiţi pentru a demonstra un rezultat fundamental.

Teorema 2.4 (*a factorilor invarianţi*). *Dacă* $A \in M_{m\times n}(\mathbb{Z})$, *atunci există* $\delta_1, \delta_2, \ldots \delta_r \in \mathbb{Z}$, $\delta_i > 0$, $1 \leqslant i \leqslant r$, *unic determinaţi, astfel încît*

$$A \sim \begin{pmatrix} \delta_1 & & & & \\ & \delta_2 & & & \\ & & \ddots & & \\ & & & \delta_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix},$$

unde $r \leqslant \min\{m, n\}$ *şi* $\delta_1 \mid \delta_2 \mid \ldots \mid \delta_r$.

Demonstraţie. Conform lemei 2.1, avem

$$A \sim \begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix} = D,$$

cu $d_i \in \mathbb{Z}$, $d_i > 0$, $1 \leqslant i \leqslant r$. Uzînd la nevoie de permutări de linii (coloane), putem presupune că $d_1 \leqslant d_2 \leqslant \ldots \ldots \leqslant d_r$.

Dacă pentru $i < j$ numărul d_i nu divide d_j, atunci conform lemei 2.3 există matricele unimodulare

$$U = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, \qquad V = \begin{pmatrix} p & q \\ s & t \end{pmatrix},$$

Scanned with OKEN Scanner

astfel încît

$$U\begin{pmatrix} d_i & 0 \\ 0 & d_j \end{pmatrix} V = \begin{pmatrix} (d_i, d_j) & 0 \\ 0 & [d_i, d_j] \end{pmatrix}.$$

Definind matricele de ordin m, respectiv n:

$$U^* = \begin{array}{c} \begin{matrix} & & i & & j & \end{matrix} \\ \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ \cdots & \cdots & x & \cdots & y & \cdots \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \\ \cdots & \cdots & z & \cdots & w & \cdots \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \end{matrix} \end{array},$$

$$V^* = \begin{array}{c} \begin{matrix} & & i & & j & \end{matrix} \\ \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ \cdots & \cdots & p & \cdots & q & \cdots \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \\ \cdots & \cdots & s & \cdots & t & \cdots \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \end{matrix} \end{array}$$

elementele nespecificate fiind egale cu 0, avem $U^* \in GL_m(\mathbb{Z})$, $V \in GL_n(\mathbb{Z})$, iar matricea UDV se obține din D înlocuind pe d_i și d_j cu (d_i, d_j), respectiv $[d_i, d_j]$.

Dacă $d_1 | d_j$, $j = 2, \ldots, r$, atunci se definește $\delta_1 = d_1$. Dacă există $j \geqslant 2$ astfel încît d_1 nu divide pe d_j, atunci d_1 se înlocuiește ca mai sus cu (d_1, d_2) și d_j cu $[d_1, d_j]$ și observăm că în acest caz $(d_1, d_2) < d_1$ și $(d_1, d_2) | [d_1, d_2]$.

Scanned with OKEN Scanner

După un număr finit de pași se ajunge ca

$$A \sim \begin{pmatrix} d'_1 & & & & \\ & d'_2 & & & \\ & & \ddots & & \\ & & & d'_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

cu $d'_1 | d'_j$, $2 \leqslant j \leqslant r$ și se ia $\delta_1 = d'_1$. Dacă $d'_2 | d'_j$, $3 \leqslant j \leqslant r$, atunci luăm $\delta_2 = d'_2$. În caz contrar, se aplică procedeul de mai sus ș.a.m.d. Astfel, după un număr finit de pași, se obține o matrice de forma celei din enunț și care este echivalentă cu A.

Unicitatea numerelor r, δ_1, δ_2, ..., δ_r se poate demonstra observînd că dacă $A \sim B$, atunci

$$\Delta_i(A) = \Delta_i(B), \quad i = 1, 2, \ldots$$

unde $\Delta_i(A)$ [respectiv $\Delta_i(B)$] este cel mai mare divizor comun al minorilor de ordin i ai matricei A (respectiv B) și că pentru matricea

$$D = \begin{pmatrix} \delta_1 & & & & \\ & \delta_2 & & & \\ & & \ddots & & \\ & & & \delta_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}, \qquad \delta_1 | \delta_2 | \ldots | \delta_r,$$

avem

$$\Delta_1(D) = \delta_1,$$
$$\Delta_2(D) = \delta_1\delta_2,$$
$$\ldots\ldots\ldots$$
$$\Delta_r(D) = \delta_1\delta_2 \ldots \delta_r,$$
$$\Delta_i(D) = 0, \quad r \leqslant i \leqslant \min\{m, n\}.$$

Scanned with OKEN Scanner

Dacă $A \in M_{mn}(\mathbb{Z})$, atunci matricea unic determinată

$$D = \begin{pmatrix} \delta_1 & & & & \\ & \delta_2 & & \mathbf{0} & \\ & & \ddots & & \\ & \mathbf{0} & & \delta_r & \\ & & & & \mathbf{0} \end{pmatrix}, \qquad \delta_1 | \delta_2 | \ldots | \delta_r,$$

astfel încît $A \sim D$, se numeşte *forma diagonal canonică a lui* A. Numerele $\delta_i > 1$ se numesc *factori invarianţi* ai matricei A.

Exemplu. Să găsim forma diagonal canonică a matricei:

$$A = \begin{pmatrix} 6 & 2 & -12 & 8 \\ -6 & 0 & 12 & -6 \\ 12 & 2 & -24 & 14 \end{pmatrix}.$$

Înmulţind pe rînd la dreapta matricea A cu matricele P_{12}, $T_{12}(-3)$, $T_{13}(6)$, $T_{14}(-4)$ de ordin patru şi apoi la stînga cu matricea $T_{31}(-1)$ de ordin trei, obţinem matricea

$$B = T_{31}(-1) A P_{12} T_{12}(-3) T_{13}(6)\, T_{14}(-4) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -6 & 12 & -6 \\ 0 & 6 & -12 & 6 \end{pmatrix}.$$

Înmulţind la stînga matricea B cu matricea D_2 de ordin trei, apoi la dreapta pe rînd cu matricele $T_{23}(2)$, $T_{24}(-1)$ de ordin patru şi în sfîrşit la stînga cu matricea $T_{32}(-1)$ de ordin trei, obţinem

$$D = T_{32}(-1)\, D_2 B\, T_{23}(2)\, T_{24}(-1) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

ceea ce reprezintă forma diagonal canonică a matricei A, 2 şi 6 fiind factorii invarianţi ai acesteia.

Fie

$$U = T_{32}(-1)\, D_2\, T_{31}(-1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$$

Scanned with OKEN Scanner

și

$$V = P_{12}T_{12}(-3)T_{13}(6)T_{14}(-4)\ T_{23}(2)\ T_{24}(-1) = \begin{pmatrix} 0 & 1 & 2 & -1 \\ 1 & -3 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Avem $U \in GL_3(\mathbb{Z})$, $V \in GL_4(\mathbb{Z})$ și

$$UAV = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

§ 3. Soluții întregi ale unui sistem de ecuații liniare

Vom studia în acest paragraf sistemele liniare cu m ecuații în n necunoscute

$$\left.\begin{aligned} a_{11}X_1 + a_{12}X_2 + \ldots + a_{1n}X_n &= b_1 \\ a_{21}X_1 + a_{22}X_2 + \ldots + a_{2n}X_n &= b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{m1}X_1 + a_{m2}X_2 + \ldots + a_{mn}X_n &= b_m \end{aligned}\right\} \qquad (S)$$

cu coeficienți a_{ij}, $b_i \in \mathbb{Z}$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$. Prin *soluția întreagă* a sistemului (S) se înțelege un sistem $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ de numere întregi λ_j, $1 \leqslant j \leqslant n$, astfel încît

$$\sum_{j=1}^{n} a_{ij}\lambda_j = b_i, \quad 1 \leqslant i \leqslant m.$$

Dacă adoptăm notațiile

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}, \quad L = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}, \quad X = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix},$$

Scanned with OKEN Scanner

atunci sistemul (S) se scrie condensat sub forma

$$AX = L.$$

Dacă $U \in GL_n(\mathbb{Z})$, $U = (u_{ij})$, atunci transformarea

$$X_i = \sum_{j=1}^{n} u_{ij} Y_j, \quad 1 \leqslant i \leqslant n,$$

sau mai condensat

$$X = U Y$$

se numeşte *substituţia întreagă unimodulară*, unde

$$Y = \begin{pmatrix} Y_1 \\ Y_2 \\ \cdot \\ \cdot \\ Y_n \end{pmatrix}.$$

Propoziţia 3.1. *Fie* $U \in GL_n(\mathbb{Z})$, $U = (u_{ij})$ *şi numerele reale* λ_j, μ_j, $1 \leqslant j \leqslant n$, *astfel încît*

$$\lambda_i = \sum_{j=1}^{n} u_{ij} \mu_j, \quad 1 \leqslant i \leqslant n.$$

Atunci $\lambda_i \in \mathbb{Z}$, $1 \leqslant i \leqslant n$, *dacă şi numai dacă* $\mu_j \in \mathbb{Z}$, $1 \leqslant j \leqslant n$. *Mai mult,* $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ *este o soluţie întreagă a sistemului* $AX = L$ *dacă şi numai dacă* $(\mu_1, \mu_2, \ldots, \mu_n)$ *este o soluţie întreagă a sistemului* $(AU)Y = L$.

Demonstraţie. Dacă $\mu_j \in \mathbb{Z}$, $i \leqslant j \leqslant n$, atunci

$$\lambda_i = \sum_{j=1}^{n} u_{ij}\mu_j \in \mathbb{Z}, \quad 1 \leqslant i \leqslant n.$$

Scanned with OKEN Scanner

Reciproc, presupunem că $\lambda_i \in \mathbb{Z}$, $1 \leqslant i \leqslant n$. Fie $V \in GL_n(\mathbb{Z})$ astfel încît $VU = UV = E$. Avem

$$\begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{pmatrix} = VU \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{pmatrix} = V \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} v_{1i}\lambda_i \\ \sum_{i=1}^{n} v_{2i}\lambda_i \\ \vdots \\ \sum_{i=1}^{n} v_{ni}\lambda_i \end{pmatrix},$$

de unde $\mu_j \in \mathbb{Z}$, $1 \leqslant j \leqslant n$. Ultima afirmaţie din propoziţie este evidentă.

Lema 3.2. *Dacă $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, atunci există $U \in GL(\mathbb{Z})$ astfel încît*

$$(a_1, a_2, \ldots, a_n)U = (d, 0, \ldots, 0),$$

unde d este c.m.m.d.c. al numerelor $a_1, a_2, \ldots, a_n$.

Demonstraţie. Arătăm mai întîi că lema este adevărată pentru $n = 2$. Fie d c.m.m.d.c. al numerelor a_1 şi a_2. Avem

$$a_1 = da_1', \quad a_2 = da_2' \text{ cu } a_1', a_2' \in \mathbb{Z}.$$

Există $h, k \in \mathbb{Z}$ astfel încît $ha_1' + ka_2' = 1$ şi fie

$$U = \begin{pmatrix} h & -a_2' \\ k & a_1' \end{pmatrix}.$$

Cum $\det U = ha_1' + ka_2' = 1$, rezultă că $U \in GL_2(\mathbb{Z})$. Avem

$$(a_1, a_2)\,U = (ha_1 + ka_2, -a_1a_2' + a_2a_1') = (d, 0).$$

Presupunem că $n > 2$ şi că lema este adevărată pentru $n - 1$. Atunci există $V_1 \in GL_{n-1}(\mathbb{Z})$ astfel încît

$$(a_2, a_3, \ldots, a_n)V_1 = (d_1, 0, \ldots, 0),$$

unde d_1 este c.m.m.d.c. al numerelor $a_2, a_3, \ldots, a_n$. Dacă

$$V = \begin{pmatrix} 1 & 0 \\ 0 & V_1 \end{pmatrix},$$

atunci $V \in GL_n(\mathbb{Z})$ şi

$$(a_1, a_2, \ldots, a_n)\, V = (a_1, d_1, 0, \ldots, 0).$$

Conform primei părţi a demonstraţiei, există $W_1 \in GL_2(\mathbb{Z})$ astfel încît

$$(a_1, d_1)\, W_1 = (d, 0),$$

unde d este c.m.m.d.c. al numerelor a_1 şi d_1. Fie

$$W = \begin{pmatrix} W_2 & 0 \\ 0 & I_{n-2} \end{pmatrix}$$

şi avem $W \in GL_n(\mathbb{Z})$. Dacă $U = VW$, atunci

$$(a_1, a_2, a_3, \ldots, a_n)\, U = (d, 0, 0, \ldots, 0).$$

Demonstraţia lemei se încheie observînd că d coincide cu c.m.m.d.c. al numerelor $a_1, a_2, \ldots, a_n$.

Teorema următoare dă un răspuns complet privind existenţa şi modalitatea de determinare a soluţiilor întregi ale ecuaţiei liniare

$$a_1X_1 + a_2X_2 + \ldots + a_nX_n = b,$$

unde $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$.

Teorema 3.3. *Ecuaţia cu coeficienţi întregi*

$$a_1X_1 + a_2X_2 + \ldots + a_nX_n = b \qquad (6.1)$$

admite soluţii întregi dacă şi numai dacă $d \mid b$, unde d este c.m.m.d.c. al numerelor $a_1, a_2, \ldots, a_n$. Dacă $U \in GL_n(\mathbb{Z})$, $U = (u_{ij})$, este astfel încît

$$(a_1, a_2, \ldots, a_n)\, U = (d, 0, \ldots, 0),$$

atunci $(\lambda_1^0, \lambda_2^0, \ldots, \lambda_n^0)$, *unde*

$$\lambda_i^0 = u_{i1}\frac{b}{d}, \qquad 1 \leqslant i \leqslant n,$$

este o soluție întreagă particulară a ecuației (6.1). *Sistemu de numere întregi* $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ *este soluție întreagă a ecuației* (6.1) *dacă și numai dacă*

$$\lambda_i = \lambda_i^0 + \sum_{j=2}^{n} u_{ij}\, t_j, \quad t_j \in \mathbb{Z}, \quad 1 \leqslant i \leqslant n, \quad 2 \leqslant j \leqslant n.$$

Demonstrație. Fie $U \in GL_n(\mathbb{Z})$ ca în enunțul teoremei. Făcînd substituția întreagă unimodulară $X = UY$, obținem

$$(d, 0, \ldots, 0)\, Y = b.$$

Evident, ultima ecuație admite soluție întreagă dacă și numai dacă $d \mid b$. O soluție întreagă particulară a acesteia este $\left(\frac{b}{d}, 0, \ldots, 0\right)$, iar soluția întragă generală este $\left(\frac{b}{d}, t_2, \ldots, t_n\right)$ cu t_j, $2 \leqslant j \leqslant n$, numere întregi arbitrare. Conform propoziției 3.1 obținem că

$$\begin{pmatrix} \lambda_1^0 \\ \lambda_2^0 \\ \vdots \\ \lambda_n^0 \end{pmatrix} = U \begin{pmatrix} \frac{b}{d} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{u_{11}b}{d} \\ \vdots \\ \frac{u_{n1}b}{d} \end{pmatrix}$$

este soluția întreagă generală a ecuației (6.1) iar

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = U \begin{pmatrix} \frac{b}{d} \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} \frac{u_{11}b}{d} + \sum_{j=2}^{n} u_{1j}t_j \\ \vdots \\ \frac{u_{n1}b}{d} + \sum_{j=2}^{n} u_{rj}t_j \end{pmatrix}.$$

Scanned with OKEN Scanner

Observaţii. 1. Cînd $d \mid b$, descrierea soluţiilor întregi ale ecuaţiei (6.1) din enunţul teoremei precedente se face cu ajutorul matricei unimodulare U. Calculul lui U se poate face folosind de $n-1$ ori algoritmul lui Euclid extins. Într-adevăr, determinăm succesiv cu acest algoritm:

$$\begin{aligned} d_1 &= (a_{n-1}, a_n), & h_1 a_{n-1} + k_1 a_n &= d_1, \\ d_2 &= (a_{n-2}, d_1), & h_2 a_{n-2} + k_2 d_1 &= d_2, \\ &\cdots\cdots\cdots & &\cdots\cdots\cdots\cdots \\ d = d_{n-1} &= (a_2, d_{n-2}), & h_{n-1} a_1 + k_{n-1} d_{n-2} &= d_{n-1} = d \end{aligned}$$

şi atunci avem

$$U = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & 1 & \\ & h_1 \; -a_n & \\ 0 & k_1 \quad a'_{n-1} & \end{pmatrix} \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ & & h_2 \; -d'_1 & \\ 0 & & k_2 \quad a'_{n-1} & \\ & & & 1 \end{pmatrix} \cdots \begin{pmatrix} h_{n-1} - d'_{n-1} & 0 \\ k_{n-1} \quad a'_1 & \\ 0 \quad 1 & \\ & \ddots \\ & 0 \end{pmatrix},$$

unde $a_n = d_1 a'_n$, $a_{n-1} = d_1 a'_{n-1}$, $d_1 = d_2 d'_1$, $a_{n-2} = d_2 a'_{n-2}$ etc.

2. Cînd $n = 2$, rezultatul teoremei 3.3 coincide cu cel stabilit în § 4, cap. V.

Lema 3.4. *Fie* $A = (a_{ij}) \in M_n(\mathbb{Z})$ *astfel încît*

$$\Delta = \det A > 0.$$

Atunci există $U \in GL_n(\mathbb{Z})$ *astfel încît*

$$AU = \begin{pmatrix} c_{11} & 0 & \ldots & 0 \\ c_{21} & c_{22} & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{pmatrix}$$

unde $c_{ii} > 0$, $1 \leqslant i \leqslant n$, *şi*

$$0 \leqslant c_{i1}, \; c_{i2}, \ldots, c_{i,i-1} < c_{ii}, \qquad 1 \leqslant i \leqslant n.$$

Demonstraţie. Fie c_{11} c.m.m.d.c. al numerelor $a_{11}, a_{12}, \ldots, a_{1n}$. Conform lemei 3.2 există $U_1 \in GL_n(\mathbb{Z})$ astfel încît

$$(a_{11}, a_{12}, \ldots, a_{1n})\, U_1 = (c_{11}, 0, \ldots, 0)$$

şi deci

$$AU_1 = \begin{pmatrix} c_{11} & 0 & \dots & 0 \\ a'_{21} & a'_{22} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots \\ a'_{n1} & a'_{n2} & \dots & a'_{nn} \end{pmatrix}$$

unde $a'_{ij} \in \mathbb{Z}$. Aplicînd din nou lema 3.2, găsim $V \in GL_{n-1}(\mathbb{Z})$ astfel încît

$$(a'_{22}, a'_{23}, \dots, a'_{2n})\, V = (c_{22}, 0, \dots, 0),$$

unde c_{22} este c.m.m.d.c. al numerelor $a'_{22}, a'_{23}, \dots, a'_{2n}$. Punînd

$$U_2 = \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix},$$

avem $U_2 \in GL_n(\mathbb{Z})$ și se obține

$$AU_1U_2 = \begin{pmatrix} c_{11} & 0 & 0 & \dots & 0 \\ a''_{21} & c_{22} & 0 & \dots & 0 \\ a''_{31} & a''_{32} & a''_{33} & \dots & a''_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a''_{n1} & a''_{n2} & a''_{n3} & \dots & a''_{nn} \end{pmatrix}$$

Dacă $0 \leqslant a''_{21} < c_{22}$, luăm $c_{21} = a''_{21}$. În caz contrar, scriem

$$a''_{21} = c_{22}q_{21} + r_{21},\ 0 \leqslant r_{21} < c_{22}.$$

Atunci

$$AU_1U_2T_{21}(-q_{21}) = \begin{pmatrix} c_{11} & 0 & \dots & 0 \\ r_{21} & c_{22} & \dots & 0 \\ & \ddots & \ddots & \\ & & \ddots & \end{pmatrix}$$

Scanned with OKEN Scanner

și luăm $c_{21} = r_{21}$. Continuînd, se găsește matricea

$$U = U_1 U_2 \ldots \in GL_n(\mathbb{Z}),$$

astfel încît matricea AU este de forma celei din enunțul lemei.

Cum inelele de clase de resturi $\mathbb{Z}_m$ sînt finite, rezultatul din teorema următoare ne permite să recunoaștem printr-un număr finit de încercări dacă sistemul din enunțul teoremei admite soluții întregi.

Teorema 3.5. *Fie un sistem de n ecuații liniare cu n necunoscute :*

$$\sum_{j=1}^{n} a_{ij} X_j = b_i, \qquad 1 \leqslant i \leqslant n, \tag{6.2}$$

astfel încît $a_{ij}, b_i \in \mathbb{Z}$ *și* $\det(a_{ij}) = \Delta > 0$. *Condiția necesară și suficientă ca sistemul* (6.2) *să admită o soluție întreagă este ca congruențele*

$$\sum_{j=1}^{n} a_{ij} X_j \equiv b_i \pmod{m}, \qquad 1 \leqslant i \leqslant n, \tag{6.3}$$

să fie solubile (în $\mathbb{Z}$) *pentru orice* $m \in \mathbb{Z}$, $0 < m \leqslant \Delta$.

Demonstrație. Evident, dacă $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ este o soluție întreagă a sistemului (6.2), atunci

$$\sum_{j=1}^{n} a_{ij} \lambda_j \equiv b_i \pmod{m}, \qquad 1 \leqslant i \leqslant n,$$

oricare ar fi $m \in \mathbb{Z}$, în particular pentru $m \in \mathbb{Z}$, $0 < m \leqslant \Delta$.

Reciproc, presupunem că (6.3) este adevărat, ceea ce se mai scrie

$$AX \equiv L \pmod{m}, \qquad 0 < m \leqslant \Delta.$$

Dacă $X = UY$ este o substituție întreagă unimodulară, atunci

$$(AU)Y \equiv L \pmod{m}, \qquad 0 < m \leqslant \Delta.$$

Luînd $U \in GL_n(\mathbb{Z})$ egală cu matricea U din enunțul lemei 3.4, sistemul (6.2) devine

$$\left.\begin{aligned} & c_{11}\, Y_1 = b_1 \\ & c_{21} Y_1 + c_{22} Y_2 = b_2 \\ & \cdots\cdots\cdots\cdots \\ & c_{n1} Y_1 + c_{n2} Y_2 + \ldots + c_{nn} Y_n = b_n \end{aligned}\right\}$$

Evident, $\Delta = c_{11}c_{22} \ldots c_{nn}$, deci

$$0 < c_{11}c_{22} \ldots c_{ii} \leqslant \Delta, \qquad 1 \leqslant i \leqslant n.$$

Cum $0 < c_{11} \leqslant \Delta$, congruența $c_{11}Y_1 = b_1 \pmod{c_{11}}$ este solubilă, deci există $h, k \in \mathbb{Z}$ astfel încît

$$c_{11}h = b_1 + kc_{11},$$

de unde $c_{11}\mu_1 = b_1$ cu $\mu_1 = h - k$.

Adunînd ecuația $c_{11}Y_1 = b_1$ înmulțită cu $-c_{21}$ cu ecuația $c_{12}Y_1 + c_{22}Y_2 = b_2$ înmulțită cu c_{11}, se obține

$$c_{11}c_{22}Y_2 = -c_{21}b_1 + c_{11}b_2.$$

Conform ipotezei, congruența

$$c_{11}c_{22}Y_2 \equiv c_{21}b_1 + c_{11}b_2 \pmod{c_{11}c_{22}}$$

este solubilă, deci există $h', k' \in \mathbb{Z}$ astfel încît

$$c_{11}c_{22}h' = -c_{21}c_{11}\mu_1 + c_{11}b_2 + k'c_{11}c_{22}.$$

Simplificînd cu $c_{11} \neq 0$, obținem

$$c_{21}\mu_1 + c_{22}\mu_2 = b_2,$$

unde $\mu_2 = h' - k' \in \mathbb{Z}$.

Scanned with OKEN Scanner

Analog, din primele trei ecuaţii în Y_1, Y_2, Y_3 obţinem

$$c_{11}c_{22}c_{33}Y_3 = c_{11}c_{22}b_3 - c_{31}c_{22}b_1 - c_{11}c_{32}b_2 + c_{21}c_{32}b_1.$$

Înlocuind $b_1 = c_{11}\mu_1$, $b_2 = c_{21}\mu_1 + c_{22}\mu_2$ şi punînd condiţia ca această ultimă ecuaţie să fie solubilă modulo $c_{11}c_{22}c_{33}$, găsim $\mu_3 \in \mathbb{Z}$ astfel încît

$$c_{31}\mu_1 + c_{32}\mu_2 + c_{33}\mu_3 = b_3.$$

Continuînd în acest fel, găsim o soluţie întreagă $(\mu_1, \mu_2, \ldots, \mu_n)$ a sistemului $AUY = L$ şi atunci $(\lambda_1, \lambda_2, \ldots, \lambda_n)$, unde

$$\lambda_i = \sum_{j=1}^{n} u_{ij}\mu_j, \qquad 1 \leqslant i \leqslant n,$$

este o soluţie întreagă a sistemului $AX = L$.

Pentru sisteme omogene de ecuaţii liniare avem un rezultat mai precis.

Teorema 3.6. *Sistemul de ecuaţii liniare*

$$\sum_{j=1}^{n} a_{ij}X_j = 0, \qquad 1 \leqslant i \leqslant m,$$

cu $a_n \in \mathbb{Z}$, $m < n$, *admite o soluţie întreagă netrivială care satisface*

$$|\lambda_j| \leqslant (a_1 a_2 \ldots a_m)^{\frac{1}{n-m}}, \quad 1 \leqslant j \leqslant n,$$

unde

$$a_i = \sum_{j=1}^{n} |a_{ij}|, \qquad 1 \leqslant i \leqslant m.$$

Demonstraţie. Fie

$$L_i(X_1, \ldots, X_n) = \sum_{j=1}^{n} a_{ij}X_j, \qquad 1 \leqslant i \leqslant m,$$

$$b_i = \sum_{a_{ij}>0} a_{ij}, \quad -c_i = \sum_{a_{ij}<0} a_{ij}, \quad 1 \leqslant i \leqslant m.$$

Atunci

$$a_i = b_i + c_i, \qquad 1 \leqslant i \leqslant m.$$

Fie a un număr întreg pozitiv. Dacă $\xi_1, \xi_2, \ldots, \xi_n$ sînt numere întregi astfel încît $0 \leqslant \xi_j \leqslant a$, atunci

$$-c_i a \leqslant L_i(\xi_1, \xi_2, \ldots, \xi_n) \leqslant b_i a, \quad 1 \leqslant i \leqslant m,$$

și deci $L_i(\xi_1, \xi_2, \ldots, \xi_n)$ ia cel mult $a_i a + 1$ valori întregi. Luînd

$$a = \left[\prod_{i=1}^{m} a_i^{\frac{1}{m-n}}\right],$$

atunci

$$a > \left(\prod_{i=1}^{m} a_i\right)^{\frac{1}{n-m}} - 1,$$

de unde

$$(a+1)^n > (a+1)^m \prod_{i=1}^{m} a_i > \prod_{i=1}^{m} (a_i a + 1).$$

Acum rezultă că există $(\xi_1', \ldots, \xi_n') \neq (\xi_1'', \ldots, \xi_n'')$ cu $0 \leqslant \xi_j', \xi_j'' \leqslant a$ astfel încît

$$L_i(\xi_1', \ldots, \xi_n') = L_i(\xi_1'', \ldots, \xi_n''), \quad 1 \leqslant i \leqslant m.$$

Definind $\lambda_i = \xi_i' - \xi_i''$, $1 \leqslant i \leqslant n$, avem

$$L_i(\lambda_1, \ldots, \lambda_n) = 0, \quad 1 \leqslant i \leqslant m,$$

$$|\lambda_j| \leqslant (a_1 \ldots a_m)^{\frac{1}{n-m}}, \quad 1 \leqslant j \leqslant n.$$

Mai mult $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$ și teorema este demonstrată.

Vom folosi acum forma diagonal canonică a matricelor din $M_{m\times n}(\mathbb{Z})$ pentru a răspunde la problema existenței și descrierii soluțiilor întregi ale unui sistem de m ecuații, cu n necunoscute și cu coeficienți întregi.

Teorema 3.7. *Fie un sistem de m ecuații liniare în n necunoscute cu coeficienți întregi*

$$\sum_{j=1}^{n} a_{ij} X_j = b_i, \quad 1 \leqslant i \leqslant n. \tag{6.4}$$

Dacă $A = (a_{ij}) \in M_{m\times n}(\mathbb{Z})$ și $U \in GL_m(\mathbb{Z}), V \in GL_n(\mathbb{Z})$, $U = (u_{ij})$, $V = (v_{ij})$, sînt astfel încît

$$UAV = \begin{pmatrix} \delta_1 & & & & \\ & \delta_2 & & O & \\ & & \ddots & & \\ & O & & \delta_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix},$$

atunci condiția necesară și suficientă ca sistemul (6.4) *să admită soluții întregi este ca*

$$\delta_k \mid \sum_{j=1}^{m} u_{kj} b_j, \quad 1 \leqslant k \leqslant r,$$

și

$$\sum_{j=1}^{m} u_{kj} b_j = 0, \quad r < j \leqslant \min\{m, n\}.$$

În aceste condiții $(\lambda_1^0, \lambda_2^0, \ldots, \lambda_n^0)$, *unde*

$$\lambda_i^0 = \sum_{k,j=1}^{r,m} \frac{v_{ik}\, u_{kj} b_j}{\delta_k}, \quad 1 \leqslant i \leqslant n,$$

este o soluție întreagă a sistemului (6.4). *Mai mult, un sistem de numere întregi* $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ *este soluție a sistemului* (6.4) *dacă și numai dacă*

$$\lambda_i = \lambda_0^i + \sum_{k=r+1}^{n} v_{ik}\, t_k, \quad t_k \in \mathbb{Z}, \quad 1 \leqslant i \leqslant n.$$

Demonstrație. Scriem sistemul (6.4) sub formă matricească, deci $AX = L$. Cum $UAVV^{-1}X = UL$, notînd cu $Y = V^{-1}X$, avem

$$DY = UL, \tag{6.5}$$

unde

$$D = \begin{pmatrix} \delta_1 & & & & \\ & \delta_2 & & \mathbf{0} & \\ & & \ddots & & \\ & & & \delta_r & \\ & \mathbf{0} & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}.$$

Acum rezultă că

$$\delta_k\, Y_k = \sum_{j=1}^{m} u_{jk}\, b_j, \quad 1 \leqslant k \leqslant r,$$

și

$$0 = \sum_{j=1}^{m} u_{kj}\, b_j, \quad r < k \leqslant \min\{m, n\}.$$

Este clar că $DY = UL$ admite soluție întreagă dacă și numai dacă

$$\delta_k \mid \sum_{j=1}^{m} u_{kj}\, b_j, \quad 1 \leqslant k \leqslant r,$$

şi o soluţie particulară a sistemului (6.5) este

$$\left(\sum_{j=1}^{m} \frac{u_{1j} b_j}{\delta_1}, \ldots, \sum_{j=1}^{m} \frac{u_{rj}\, b_j}{\delta_r}, 0, \ldots, 0 \right)$$

iar soluţia generală a lui (6.5) este

$$\left(\sum_{j=1}^{m} \frac{u_{1j}\, b_j}{\delta_1}, \ldots, \sum_{j=1}^{m} \frac{u_{rj}\, b_j}{\delta_r}, t_{r+1}, \ldots, t_n \right)$$

cu $t_{r+1}, \ldots, t_n$ arbitrare din $\mathbb{Z}$.

Întrucît $X = VY$, rezultă că soluţiile sistemului (6.4) sînt cele din enunţ.

De exemplu, să găsim, în caz că există, soluţiile întregi ale sistemului

$$\left.\begin{aligned} 6X_1 + 2X_2 - 12X_3 + 8X_4 &= 10 \\ -6X_1 + 12X_3 - 6X_4 &= 18 \\ 12X_1 + 2X_2 - 24X_3 + 14X_4 &= -8 \end{aligned}\right\} \tag{6.6}$$

Avem

$$A = \begin{pmatrix} 6 & 2 & -12 & 8 \\ -6 & 0 & 12 & -6 \\ 12 & 2 & -24 & 14 \end{pmatrix}.$$

Din exemplul de la § 2 rezultă că

$$UAV = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

unde

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 1 & 2 & -1 \\ 1 & -3 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Avem $r = 2$, $\delta_1 = 2$, $\delta_2 = 6$. Din

$$\sum_{j=1}^{3} u_{1j} b_j = 10 \quad \text{și} \quad 2 \mid 10, \quad \text{unde } 2 = \delta_1,$$

$$\sum_{j=1}^{3} u_{2j} b_j = -18 \quad \text{și} \quad 6 \mid -18, \quad \text{unde } 6 = \delta_2,$$

$$\sum_{j=1}^{3} u_{3j} b_j = 0$$

rezultă că sistemul (6.6) admite soluții întregi. Urmînd descrierea dată soluțiilor întregi în teorema 3.7, găsim că

$$(\lambda_1^0, \lambda_2^0, \lambda_3^0, \lambda_4^0) = (-3, 14, 0, 0)$$

iar soluția întreagă generală este

$$\lambda_1 = -3 + 2t_3 - t_4, \quad \lambda_2 = 14 - t_4, \quad \lambda_3 = t_3, \quad \lambda_4 = t_4,$$

unde t_3 și t_4 sînt numere întregi arbitrare.

Scanned with OKEN Scanner

BIBLIOGRAFIE

1. Albu, T. și Ion, I. D. *Capitole de teoria algebrică a numerelor*. Tipografia Universității din București, 1978.
2. Borel, E. *Les nombres premiers*. Paris, 1958.
3. Cognac, G., Thiberge, L., *Mathématiques élémentaires (Arithmétique Algebre)*. Paris Masson et Cie, Editeurs, 1963.
4. Creangă, I. ș. a. *Introducere în teoria numerelor*. București, Editura didactică și pedagogică, 1965.
5. Golstein, E., Youdine, D. *Problèmes particuliers de la programmation linéaire*. Moscou, Mir, 1973.
6. Ion, I. D., Zidăroiu, C., Popoviciu, N. *Elemente de algebră și programare liniară*. București, Editura didactică și pedagogică, 1972.
7. Ion, I. D. *Elemente de aritmetică pentru învățământul liceal*.. În: Matematica în liceu, II, pag. 117—130, București, 1976.
8. Ion I. D., Radu, N. *Algebra*, București, Editura didactică și pedagogică, 1975.
9. Jacobson, N. *Basic Algebra* I. San Francisco, Freeman, 1974.
10. Kalujnin, L. A. Vvedenie v obsciuiu *aghebru*. Moscova, Nauka, 1973.
11. Kaufmann, A. Henry-Labordère, A. *Metode și modele ale cercetării operaționale*. București, Editura științifică și enciclopedică, 1975.
12. Knuth, E. D. *The art of computer programming*, I, II. Addison-Wesley Publishing Company, 1969.
13. Mac Lane, S., Birkhoff, G. *Algebra*. MacMillan Company, 1969.
14. Mordell. J. L. *Diophantine equations*. New York, Academic Press, 1969.
15. Niță, C., Spircu, T. *Probleme de structuri algebrice*. București, Editura tehnică, 1974.
16. Popovici, C. P. *Calculatoare cu program și teoria programării*. București, Editura științifică, 1972.
17. Popovici, C. P. *Logică și teoria numerelor*, București, Editura didactică și pedagogică, 1970.
18. Sierpinski, W. *A selection of problems in the theory of numbers*. Oxford, Pergamon Press, 1966.
19. Yaglom, I., Trakhtenbrot, B., Ventsel, H., Solodovnicov, A. *Nouvelles orientations des mathématiques*. Moscou, Mir, 1975.

Scanned with OKEN Scanner

VOR APĂREA:

NICULA, GH.
Funcţii spline şi aplicaţii

Acad. TEODORESCU, N., OLARIU, V.
Ecuaţii diferenţiale şi cu derivate parţiale, Vol. I

POPESCU, M., BOJU, V.
Probleme de geometria varietăţilor diferenţiabile

VRĂNCEANU, GH. GH., MITITELU, ST.
Probleme de cercetare operaţională

Scanned with OKEN Scanner

Redactor: VALENTINA CREȚU
Tehnoredactor: ELENA GERU
Coperta — Supracoperta: MARIANA NEGRU

Bun de tipar: 27.04.1978. Coli de tipar 14,5
Tiraj: 12200+20+65 exemplare legate. C.Z. 511.681.14

C. 1505. — I. P. INFORMAȚIA
str. Brezoianu nr. 23—25
București

Scanned with OKEN Scanner